GROWTH OF ALGEBRAS AND CODES

A Dissertation

by

DİLBER KOÇAK

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Rostislav Grigorchuk
Committee Members,	Sergiy Butenko
	Zoran Šunić
	Yaroslav Vorobets
Head of Department,	Emil Straube

August 2016

Major Subject: Mathematics

ABSTRACT

This dissertation is devoted to the study of the growth of algebras and formal languages. It consists of three parts.

The first part is devoted to the growth of finitely presented quadratic algebras. The study of these algebras was motivated by the question about the growth types of Koszul algebras which are a special subclass of finitely presented quadratic algebras. We show that there exist finitely presented quadratic algebras of intermediate growth and give two concrete examples of such algebras with their presentations.

The second part focuses on the study of the growth of metabelian Lie algebras and their universal enveloping algebras. Our motivation was to construct finitely presented algebras of different intermediate growth types. As an outcome of this investigation we prove that for any $d \in \mathbb{N}$ there exists a finitely presented algebra whose growth function is equivalent to $e^{n^{d/(d+1)}}$.

The last part focuses on infinite codes over finite alphabets, their properties and growth. A special attention is paid to S-codes, weak S-codes and Markov codes which play an important role in coding theory and ergodic theory. We investigate what types of codes may have maximal growth. Also, we prove that S-codes covering Bernoulli schemes are maximal.

DEDICATION

To my big, colorful and joyful family

ACKNOWLEDGEMENTS

First, I would like to present my deep gratitude and thanks to my advisor *Rostislav Ivanovich Grigorchuk* for his constant support, invaluable guidance and encouragements throughout my doctoral studies at Texas A&M University.

I would like to thank the committee members Zoran Šunić and Yaroslav Vorobets for their help and stimulating suggestions.

The kind members of the Department of Mathematics were helpful throughout the last six years.

Special thanks go to Mahmut Kuzucuoğlu for his support during and after my years in METU.

I also wish to express my deepest thanks to my family for their love, care and support.

There are many friends to whom I wish to send my thanks for their friendship throughout the years.

Finally, my biggest thanks goes to the best thing that happened to me in College Station, my beloved husband. His love, constant support and patience were essential to complete this work.

The author acknowledges partial support from TUBITAK during the years in METU and also NSF grant DMS-1207699.

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

1. INTRODUCTION

The notion of growth has various applications in different areas of mathematics. Although it was studied for a long time in some branches of mathematics such as geometry and analysis, its introduction to algebra is rather new. In vague terms, the growth could be summarized as follows: Given an algebraic structure (e.g., a group, an algebra, a formal language) one can consider this structure as a union of finite parts and measure the sizes of these parts by assigning a number to each. Out of this process one obtains a monotone increasing function which measures how fast these parts grow to form the whole structure. It is of great interest in various areas of mathematics to describe the growth rate of such functions, in particular growth functions of algebraic structures.

The growth rate is a useful invariant for algebraic structures such as groups and algebras. The notion of growth function for groups was introduced by A. S. Švarc [Šva55] and independently by J. Milnor [Mil68a]. Their motivations were mainly geometric and topological. The study of the growth of algebras dates back to the papers by I. M. Gelfand and A. A. Kirillov [GK66b, GK66a] who in particular introduced the notion which is now called the Gelfand-Kirillov dimension. The first systematic development of the properties of the Gelfand-Kirillov dimension and the growth of algebras appears in a paper of W. Borho and H. Kraft [BK76].

Growth types of algebraic structures splits into three main classes: Polynomial, exponential or intermediate (i.e., between polynomial and exponential). Group growth was studied by many authors such as J. Milnor [Mil68b], J. Wolf [Wol68], Y. Guivarc'h [Gui70], H. Bass [Bas72], B. Hartly. The description of groups of polynomial growth was obtained by M .Gromov in his celebrated work [Gro81]. He

proved that every finitely generated group of polynomial growth is virtually nilpotent. The situation for algebras is rather different from groups. M. Smith [Smi76] established the existence of virtually solvable Lie algebras whose universal enveloping algebras have superpolynomial growth. Later A. I. Lichtman and V. A. Ufnarovskiĭ [Lic84, LU95] investigated growth rates of finitely generated solvable Lie algebras and their universal enveloping algebras.

For a while it was an open question if there are algebras and (semi)groups of intermediate growth. V. E. Govorov gave the first examples of finitely generated semigroups and associative algebras of intermediate growth in [Gov72]. More examples of associative algebras and Lie algebras of intermediate growth can be found in [She80, Ufn80, KKM83, Pet93]. The first examples of finitely generated groups of intermediate growth were constructed by R. I. Grigorchuk [Gri83, Gri84]. These examples are basically the only source of groups of intermediate growth and established various research directions in the theory of groups. After that the question of the existence of finitely presented groups and algebras of intermediate growth started to be among central questions. While for algebras such examples were found [Ste75, Ufn82], it remains open whether there exists a finitely presented group of intermediate growth and is considered as one of the most difficult problems of group theory.

Among finitely presented algebras, quadratic algebras (i.e., the algebras given by quadratic relations) play an important role. Koszul algebras constitute a special subclass of quadratic algebras. In [PP05], it was conjectured that Koszul algebras have either polynomial or exponential growth.

Although there are examples of finitely presented algebras of intermediate growth, very little is known about their intermediate growth types. It is still an open problem whether there exist finitely presented algebras of intermediate growth less than $e^{\sqrt{n}}$.

Examples of finitely generated semigroups and algebras of such growth can be found in [LM01].

The growth of formal languages was first studied by M. P. Schutzenberger. Special attention is paid on certain type of languages called codes. There are various kinds of codes such as S-codes, weak S-codes and Markov codes that play an important role in coding theory, information theory and ergodic theory. Particular studies of the growth of these codes and their use in different areas of mathematics can be found in many works such as [Meš59, BH63, Lev64, Zas64, Mar70, Liv74, GS82, BP85].

In this dissertation, we will touch upon various points of the notion of growth of associative algebras, Lie algebras and infinite codes. The results are discussed in three main chapters, each having its own short introduction into the history of the problem under consideration.

The dissertation is organized as follows: Chapter 2 contains preliminaries and background on various topics related to the material that will be discussed in the forthcoming chapters. Chapter 3 is related to the results of [Koç15]. Chapter 4 contains the results on growth of finitely presented Lie algebras. Chapter 5 is related to various classes of infinite codes over finite alphabets, their properties and growth.

2. PRELIMINARIES

This chapter contains basics and preliminaries which will be used in the main parts of the dissertation. The author tried to be as self-contained as possible.

2.1 Growth of Algebras

An algebra (not necessarily associative) over a field k is called *finitely generated* if it is a quotient of a free algebra of finite rank. Let A be a k-algebra (not necessarily associative) with finite generating set $S = \{s_1, \ldots, s_m\}$. If $A(S, 0) = k$ and for $n \geq 1$, $A(S, n)$ denotes the k-subspace of A spanned by all monomial words of length at most n in the elements of S, then

$$A = \bigcup_{n=0}^{\infty} A(S, n).$$

The *growth function* of A with respect to S is the following

$$\gamma_{S,A}(n) = dim_k(A(S, n))$$

and the formal power series

$$F_{S,A}(z) = \sum_{n=0}^{\infty} \gamma_{S,A}(n) z^n$$

is the corresponding *growth series* of A with respect to S. One also defines the *spherical growth function* of A as

$$\delta_{S,A}(n) = \gamma_{S,A}(n) - \gamma_{S,A}(n-1)$$

with $\delta_{S,A}(0) = \gamma_{S,A}(0)$, and the corresponding *spherical growth series* as

$$P_{S,A}(z) = \sum_{n=0}^{\infty} \delta_{S,A}(n) z^n = (1-z) F_{S,A}(z).$$

The growth function of an algebra depends on the choice of the generating subspace. In order to remove this dependence, we introduce the following equivalence relation.

Definition 2.1.1. Let f and g be increasing and positive valued functions on $\mathbb{N}$. Set $f \precsim g$ if and only if there exists $C \in \mathbb{N}$ such that $f(n) \leq Cg(Cn)$ for all $n \in \mathbb{N}$. If $f \precsim g$ and $g \precsim f$, f and g are equivalent functions and this equivalence is denoted by $\sim$. The corresponding equivalence class containing f is denoted by $[f]$ and it is called the *growth* of f. We set $[f] \leq [g]$ if and only if $f \precsim g$.

Remark 2.1.1. If f and g are polynomials, then $f \sim g$ if and only if f and g have the same degree.

Remark 2.1.2. For positive real numbers ϵ and η, $\epsilon < \eta$ if and only if $[2^{n^\epsilon}] < [2^{n^\eta}]$.

Remark 2.1.3. $a^n \sim b^n$ for any $a, b > 1$.

Lemma 2.1.1. *Let A be a finitely generated k-algebra with generating sets $S = \{s_1, \ldots, s_m\}$ and $S' = \{s'_1, \ldots, s'_l\}$. Then $\gamma_{S,A} \sim \gamma_{S',A}$.*

Proof. Since $A = \cup_{n=0}^{\infty} A(S,n) = \cup_{n=0}^{\infty} A(S',n)$, there exist positive integers t and u such that

$$S' \subset A(S,t) \text{ and } S \subset A(S',u).$$

Thus $\gamma_{S',A}(n) \leq \gamma_{S,A}(tn)$ and $\gamma_{S,A}(n) \leq \gamma_{S',A}(un)$ which imply $\gamma_{S,A} \sim \gamma_{S',A}$. □

The growth of a finitely generated algebra A is thus independent of the choice of the generating set. When there is no risk of confusion, we write $\gamma_A(n)$, $\delta_A(n)$, $F_A(z)$, $P_A(z)$ instead of $\gamma_{S,A}(n)$, $\delta_{S,A}(n)$, $F_{S,A}(z)$, $P_{S,A}(z)$.

Definition 2.1.2. Let A be a finitely generated k-algebra, and S, a finite generating set of A. Then $\gamma_A := [\gamma_A(n)]$ is called the *growth* of A. A is said to have

- *polynomial growth* if $\gamma_A(n) \sim n^d$ for some $d \in \mathbb{N}$
- *exponential growth* if $\gamma_A(n) \sim e^n$
- *intermediate growth* if $\gamma_A(n) \precnsim e^n$ and $n^d \precnsim \gamma_A(n)$ for any $d \in \mathbb{N}$.

A is said to have *subexponential growth* if $\gamma_A(n) \precnsim e^n$.

Definition 2.1.3. For a finitely generated k-algebra A with growth function $\gamma_A(n)$, *Gelfand-Kirillov dimension* of A is defined as

$$GKdimA = \overline{\lim_{n\to\infty}} \frac{\ln \gamma_A(n)}{\ln n} = \inf\{d \mid \gamma_A \precnsim n^d\}.$$

Example 2.1.1. For an algebra of superpolynomial growth (i.e., an algebra whose growth is greater than n^d for any $d > 0$), The Gelfand-Kirillov dimension is infinite. The Gelfand-Kirillov dimension of an algebra with polynomial growth $[n^d]$ is d.

It is clear that the growth of a finitely generated algebra A is equivalent to a constant function if A is finite dimensional. The following result, due to Borho and Kraft [BK76], shows that the exponential growth is the largest growth that an algebra can have.

Proposition 2.1.1. *If A is a finitely generated infinite dimensional algebra over k, then $n \precnsim \gamma_A(n) \precnsim e^n$.*

Example 2.1.2. Let $A = k\langle x, y\rangle$ be the free associative algebra on two generators. The growth function of A with respect to $X = \{x, y\}$ is

$$\gamma_{X,A}(n) = dim_k(A(X, n)) = 1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$$

Thus $\gamma_A(n) \sim 2^n$.

Example 2.1.3. Let L be the free Lie algebra on m generators. The growth function of L with respect to the generating set $X = \{x_1, \ldots, x_m\}$ is

$$\gamma_{X,L} = \sum_{i=1}^{n} \frac{1}{i} \sum_{d|i} \mu(d) m^{i/d} \sim m^n$$

where μ denotes the Möbius function.

Theorem 2.1.1. *Let A be either a finitely generated associative algebra or a Lie algebra.*

(i) *If A contains a free two-generated subalgebra, then the growth of A is exponential.*

(ii) *The growth of A equals to the growth of any of its subalgebras of finite index.*

Proof. See [Ufn90]. □

Remark 2.1.4. The growth of a finitely generated (semi)group is defined as the growth of its (semi)group algebra. Thus an analogue of Theorem 2.1.1 holds for (semi)groups.

Example 2.1.4. Let $A = k\langle x, y\rangle$ be the free associative algebra on two generators and I be the ideal of A generated by the monomials $x^i y^{i-1} x^i$ and $y^i x^{i-1} y^{i-1}$ for $i \in \{2, 3, \ldots\}$. Then the algebra $\bar{A} = A/I$ has intermediate growth (See [Gov72]).

Example 2.1.5. Let $A = k[x_1, x_2, \ldots, x_d]$ be the commutative polynomial algebra over k. A is the set of polynomials in variables $x_1, \ldots, x_d$ with coefficients in k. The set of variables $X = \{x_1, x_2, \ldots, x_d\}$ generates A, and it is easily verified that

$$\gamma_{X,A}(n) = dim_k(A(X, n)) = \sum_{i=0}^{n} \binom{i+d-1}{d-1} = \binom{n+d}{d}$$

is a polynomial of degree d, i.e., $\gamma_A(n) \sim n^d$.

This example shows that for any natural number d, there is a finitely generated algebra A of polynomial growth $[n^d]$. In [BK76], it was shown that the growth types of finitely generated algebras can be prescribed within a rather wide range of functions.

Theorem 2.1.2. *Let Φ denote the set of eventually monotone increasing and positive valued functions and $f : \mathbb{R} \to \mathbb{R}^+$, $f|_{\mathbb{N}}$ be a function with the following properties.*

(a) *$[f|_{\mathbb{N}}] > [n^2]$, and $g \in \Phi$ where $g(n) = f(n)/n^2$.*

(b) *The third derivative f''' exists and satisfies $0 \leq f'''(t) < 1$ for $t \geq 0$.*

Then there exists a two-generator k-algebra A with $[\gamma_A] = [f|_{\mathbb{N}}]$.

Corollary 2.1.1. *For a real number r with $2 < r \leq 3$, there exists a finitely generated algebra whose growth function is equivalent to n^r.*

With the help of Corollary 2.1.1, for any $r \geq 2$, the existence of an algebra with growth function equivalent to n^r can be shown (see, for example, [KL00]). For $1 < r < 2$ the existence problem was open until Bergman [Ber78a] showed that no algebras exist whose Gelfand-Kirillov dimension belongs to this open interval.

Theorem 2.1.3. *(Bergman's Gap Theorem) For $1 < r < 2$, there do not exist an algebra whose growth function is equivalent to n^r.*

Proof. See [KL00, Ufn82] □

Definition 2.1.4. For an algebra A with finite generating set S, the *exponential growth rate* of A with respect to S is

$$\omega_{S,A} = \lim_{n\to\infty} \sqrt[n]{\gamma_{S,A}(n)}.$$

By submultiplicative property of $\gamma_{S,A}(n)$ (i.e. $\gamma_{S,A}(n+m) \leq \gamma_{S,A}(n)\gamma_{S,A}(m)$), this limit always exists (See [Smi76]).

Remark 2.1.5. Let $\gamma_{S,A}$ and $\gamma_{S',A}$ be the growth functions of an algebra A with respect to the generating sets S and S', respectively and let $\omega_{S,A}$ and $\omega_{S',A}$ be the corresponding exponential growth rates.

(i) If A is infinite dimensional, then $\omega_{S,A} \geq 1$.

(ii) $\omega_{S,A}^{-1}$ is the radius of convergence of the growth series $F_{S,A}(z)$.

(iii) $\omega_{S,A} > 1$ implies $\omega_{S',A} > 1$.

Proposition 2.1.2. *A finitely generated algebra A with generating set S has subexponential growth if and only if $\omega_{S,A} = 1$.*

Proof. If A has subexponential growth , then for any $\epsilon > 0$, $\gamma_{S,A}(n) \precsim (1+\epsilon)^n$ which implies $\omega_{S,A} \leq 1+\epsilon$. Hence $\omega_{S,A} = 1$. If A has exponential growth then there exists $\epsilon > 0$ such that $\gamma_{S,A}(n) \succsim (1+\epsilon)^n$. Thus $\omega_{S,A} \geq 1+\epsilon$. □

2.2 Finitely Presented Graded Algebras

A *presentation* of an algebra A over a field k is a pair consisting of a free algebra F with generating set $(x_i)_{i\in I}$ and a homomorphism Π of F onto A. A family $(f_j)_{j\in J}$ in F which generates $Ker(\Pi)$ as an ideal (thus $Ker(\Pi)$ consists of polynomials of the form $g = \sum_{j\in J} c_j g_j f_j g_j{}'$ for $c_j \in k$, and $g_j, g_j{}' \in F$). One denotes such a presentation by

$$A = \langle (x_i)_{i\in I} \mid (f_j = 0)_{j\in J} \rangle.$$

A is said to be the algebra generated by $\{x_i\}_{i\in I}$ with the set of relations $\{f_j = 0\}_{j\in J}$. A *finite presentation* is one for which the sets I and J are finite; an algebra is called

finitely presented if it has a finite presentation.

A *grading* $\mathcal{A} = \{A_i\}_{i=0}^{\infty}$ of the k-algebra A is a sequence of k-subspaces A_i of A such that

$$A = \bigoplus_{i=0}^{\infty} A_i \text{ and } A_i A_j \subset A_{i+j} \text{ for all } i, j \in \mathbb{N} \cup \{0\}.$$

An algebra with a grading $\mathcal{A}$ is called $\mathcal{A}$-*graded* or simply *graded*. If each A_i is finite dimensional, then it is called *finitely graded*. Throughout this dissertation, we will be working with only the algebras which are finitely graded and assume that the zero component is k (This condition is usually called the *connectedness* of the algebra).

Let F be the free algebra of finite rank. There exists a grading $\mathcal{T} = \{T_i\}_{i=0}^{\infty}$ such that

$$F = T_0 \oplus T_1 \oplus \ldots \oplus T_n \oplus \ldots.$$

Then every $u \in F$ can be written uniquely as a sum

$$u = u_0 + u_1 + \ldots + u_k \text{ where } u_i \in T_i.$$

The elements of T_i are said to be *homogeneous of degree* i. The degree of a homogeneous element f is denoted by $deg(f)$. Let R be a set of non-zero homogeneous polynomials $f_1, f_2, \ldots$ such that $1 \leq deg(f_i) \leq deg(f_{i+1})$ and such that the number of polynomials of degree n is finite for any n. For the ideal I generated by $f_1, f_2, \ldots$, we can form the factor algebra $A = F/I$. If $r = u_1 + u_2 + \ldots + u_n \in I$, $u_i \in T_i$, then each $u_i \in I$, since I is generated by homogeneous polynomials. For the factor algebra $A = F/I$,

$$v_1 + \ldots + v_s + I = w_1 + \ldots + w_t + I, \; v_i, w_i \in T_i$$

implies $v_i + I = w_i + I$ for each i. Hence $A = A_0 \oplus A_1 \oplus \ldots \oplus A_n \oplus \ldots$, where $A_n = T_n/T_n \cap I$ and it is easily verified that $A_i A_j \subset A_{i+j}$. So, A is a graded algebra inheriting the grading of F. On the other side, for a given graded algebra A, in the light of uniqueness of decomposition into the corresponding components in A, if $u = 0$ is a relation in A, then every homogeneous summand u_n of u will also be a relation: $u_n = 0$. Therefore, in a graded algebra all the defining relations may be considered homogeneous.

Definition 2.2.1. $\mathcal{A} = \{A_i\}_{i=0}^{\infty}$ is called a *natural graduation* if the degree of a monomial coincides with the length of this monomial.

Lemma 2.2.1. *Let A be a finitely generated k-algebra with finite grading $\mathcal{A} = \{A_i\}_{i=0}^{\infty}$. Then $\delta_A(n) \sim dim_k(A_n)$.*

Proof. Let S be a finite generating set of A. Since $A = \bigoplus_{i=0}^{\infty} A_i$, there exists a positive integer m such that

$$S \subset A_0 \oplus A_1 \oplus \ldots \oplus A_m.$$

Let S' be the basis of $A_0 \oplus A_1 \oplus \ldots \oplus A_m$. Thus we can take S' as a generating set of A and

$$A(S', n) = A_0 \oplus A_1 \oplus \ldots \oplus A_{mn}$$

this means that

$$\gamma_{S',A}(n) = dim_k(A_0 \oplus A_1 \oplus \ldots \oplus A_{mn}) = \sum_{i=0}^{mn} dim_k(A_i).$$

and,

$$\delta_{S',A}(n) = \gamma_{S',A}(n) - \gamma_{S',A}(n-1) = \sum_{i=m(n-1)}^{mn} dim_k(A_i).$$

We get

$$dim_k(A_{mn}) \leq \delta_{S',A}(n) \leq m\ dim_k(A_{mn})$$

hence

$$\delta_A(n) \sim dim_k(A_n).$$

□

In view of Lemma 2.2.1, we can define the spherical growth series of a graded algebra $A = \bigoplus_{n=0}^{\infty} A_n$ as

$$H_A(z) = \sum_{n=0}^{\infty} dim_k(A_n) z^n$$

which is also called the *Hilbert series* of the algebra A.

For a while, it was conjectured that any finitely presented graded algebra should have a rational Hilbert series. However this conjecture was disproved by Shearer [She80], who produced a graded algebra with 11 generators and 77 relations which has a non-rational Hilbert series. The following theorem shows that why this is an interesting question.

Theorem 2.2.1. *If the algebra A has rational Hilbert series, then A has exponential or polynomial growth.*

Proof. See [Sta97, Theorem 4.1.1]. □

It follows from Theorem 2.2.1 that an algebra of intermediate growth cannot have rational Hilbert series. This enables to provide more examples having non-rational Hilbert series. We consider them in the following sections.

2.3 Bergman's Diamond Lemma

In this section we describe how to construct a basis for associative algebras. The first results on bases of algebras appeared in the context of Lie algebras in papers

of A.I. Shirshov [Šir62]. For the associative case, a source is a paper by L. A. Bokut [Bok76]. In this section, we state and prove the *Bergman's Diamond Lemma* [Ber78b] which is also called the *lemma on composition* in many sources (see for example [Ufn90]).

Let $\langle X\rangle$ denote the monoid generated by the set X and $k\langle X\rangle$ the free associative algebra generated by X over k. Suppose that R is a set of *relations* of the form $u = P$ where $u \in \langle X\rangle$ and $P \in k\langle X\rangle$. When the directions of the elements in R are taken into account, R is called a *rewriting system* and a relation $u = P$ is called a *reduction* denoted by $u \to P$. For $v, w \in k\langle X\rangle$, we write $v \to w$ if $v = v_1 u v_2,\ w = v_1 P v_2$ for some reduction $u \to P$ in R and $v_1, v_2 \in k\langle X\rangle$. Reflexive and transitive closure of $\to$ is denoted by $\overset{*}{\to}$. For $v, w \in k\langle X\rangle$, $v \overset{*}{\to} w$ if there exist $v_1, \ldots, v_n \in k\langle X\rangle$ such that $v \to v_1 \to \cdots \to v_n \to w$. A *semigroup partial ordering on* $\langle X\rangle$ (a partial order $\leq$ such that $B \leq B'$ implies $ABC \leq AB'C$ for $A, B, B', C \in \langle X\rangle$) is called *compatible with* R if P is a linear combination of monomials $< u$ for any $u \to P$ in R. An element $f \in k\langle X\rangle$ is called *irreducible* if every reduction leaves it unchanged. If R is *Noetherian* (i.e., there is no infinite sequence $v_1 \to v_2 \to \ldots$) and *confluent* (i.e., for any $f, g, h \in k\langle X\rangle$ such that $f \overset{*}{\to} g$ and $f \overset{*}{\to} h$ there exists $w \in k\langle X\rangle$ such that $g \overset{*}{\to} w$ and $h \overset{*}{\to} w$), then R is called a *complete rewriting system.* If R is a complete rewriting system then for any $f \in k\langle X\rangle$, there exists a unique irreducible element $a \in k\langle X\rangle$ such that $f \overset{*}{\to} a$. It is called the *irreducible form* (or *normal form*) of f and is denoted by f_{irr}. One can observe that irreducible forms of $k\langle X\rangle$ form a k-submodule which we denote by $k\langle X\rangle_{irr}$. For $f \in \langle X\rangle$, there may exist more than one reduction that can be applied to f. We call them *ambiguities* and define possible ambiguities that may appear in $\langle X\rangle$ as follows : Let R_L be the set of left-hand sides of the rules from R,

$$R_L = \{u \in \langle X\rangle \mid u \to P \in R\}.$$

There are two types of ambiguities:

(1) *overlap ambiguities*: $a = ABC \in \langle X \rangle$, where $AB,\ BC \in R_L$.

(2) *inclusion ambiguities*: $a = ABC$ for some $A, B, C \in \langle X \rangle$ and $ABC,\ B \in R_L$.

Suppose $AB \to P_1$ and $BC \to P_2$ ($ABC \to P_1$ and $B \to P_2$, respectively) if there exist $w \in k\langle X \rangle$ such that $P_1 C \xrightarrow{*} w$ and $AP_2 \xrightarrow{*} w$ ($P_1 \xrightarrow{*} w$ and $AP_2C \xrightarrow{*} w$, respectively), the overlap (the inclusion, respectively) ambiguity is called *resolvable*.

Theorem 2.3.1. *[Ber78b, Theorem 1.2] Let R be a Noetherian rewriting system for a free associative algebra $k\langle X \rangle$, and $\leq$ a semigroup partial ordering on $\langle X \rangle$, compatible with R. Then the following conditions are equivalent:*

(a) All ambiguities of R are resolvable.

(b) R is a complete rewriting system.

(c) If I is a two-sided ideal generated by $\{u - P |\ u \to P \in R\}$, the set of irreducible monomials of $\langle X \rangle$ forms a k-basis for the associative algebra $A = k\langle X \rangle / I$.

Proof. It is clear that (b) implies (a). Since R is Noetherian, every element in $k\langle X \rangle$ goes to an irreducible element. To show that (a) implies (b), it suffices to prove the uniqueness of the irreducible form for $f \in k\langle X \rangle$. Note that f has a unique irreducible form if and only if every monomial that appears in the decomposition of f has a unique irreducible form. So, without loss of generality we can assume that $f \in \langle X \rangle$. Suppose that any monomial less than f with respect to the semigroup partial ordering $\leq$ has a unique irreducible form.

Case 1. If there is no ambiguity in the presentation of f, f is of the following form

$$A_1 u_1 A_2 u_2 \dots A_n u_n A_{n+1},$$

where $u_i \in R_L$ and A_i is irreducible for $i \in \{1, 2, \ldots, n+1\}$.

$$f \to A_1 u_1 A_2 u_2 \ldots A_i P_i \ldots A_n u_n A_{n+1}$$

for any $i \in \{1, \ldots, n\}$. Since $A_1 u_1 A_2 u_2 \ldots A_i P_i \ldots A_n u_n A_{n+1} < f$, it has a unique irreducible form a and a is also irreducible form of f. For any $i \in \{1, \ldots, n\}$, we have

$$A_1 u_1 A_2 u_2 \ldots A_i P_i \ldots A_n u_n A_{n+1} \xrightarrow{*} A_1 P_1 A_2 P_2 \ldots A_i P_i \ldots A_n P_n A_{n+1}$$

and this implies

$$A_1 P_1 A_2 P_2 \ldots A_i P_i \ldots A_n P_n A_{n+1} \xrightarrow{*} a.$$

So, a is the unique irreducible form of f.

Case 2. Let $f = LABCM$ where $A, B, C, L, M \in \langle X \rangle$ and $AB \to P_1, BC \to P_2 \in R$ ($ABC \to P_1, B \to P_2 \in R$, respectively). Since all the ambiguities are resolvable, there exists $d \in k\langle X \rangle$ such that $LP_1CM \xrightarrow{*} LdM$ and $LAP_2M \xrightarrow{*} LdM$ ($LP_1M \xrightarrow{*} LdM$ and $LAP_2CM \xrightarrow{*} LdM$, respectively). Since $LdM < f$, it has a unique irreducible form a which is also irreducible form of f. By the same reason as in *Case 1*, a is the unique irreducible form for f. Now, we can prove that (b) implies (c). Define a map φ from $k\langle X \rangle$ onto $k\langle X \rangle_{irr}$:

$$\begin{array}{rccc} \varphi: & k\langle X \rangle & \to & k\langle X \rangle_{irr} \\ & f & \mapsto & f_{irr} \end{array}$$

Since every element of $k\langle X \rangle$ has a unique irreducible form, φ is well-defined. If

$\varphi(f) = 0$ then there exists $f_1, f_2, \ldots, f_n \in k\langle X\rangle$ such that

$$f \to f_1 \to f_2 \cdots \to f_n = 0$$

This implies that $f - f_1, f_1 - f_2, \ldots, f_{n-1} - f_n \in I$ and so

$$(f - f_1) + \ldots + (f_{n-1} - f_n) = x \in I \text{ and } Ker(\varphi) \subset I.$$

If f is an element of I then it is a k-linear combination of the elements of the form $A(u - P)B$ for $(u, P) \in R$ and $A, B \in k\langle X\rangle$ and $\varphi(A(u - P)B) = \varphi(AuB) - \varphi(APB) = 0$ (since R is confluent, AuB and aPB go to the same irreducible form). Hence, $I \subset Ker(\varphi)$ and we have $k\langle X\rangle / I \cong k\langle X\rangle_{irr}$. We can identify $k\langle X\rangle/I$ with the k-module $k\langle X\rangle_{irr}$, made a k-algebra by the multiplication $a \cdot b = (ab)_{irr}$. So (b) implies (c). Assume (c) is true and $f \in k\langle X\rangle$ can be reduced to two different elements b and b' in $k\langle X\rangle_{irr}$. Then $b - b' \in k\langle X\rangle_{irr} \cap I = \{0\}$. This shows that (c) implies (b) and completes the proof of Theorem 2.3.1. □

For a rewriting system R, we denote the set of irreducible monomials (or words) by $Irr(R)$ and define the growth function $\gamma_{Irr(R)}(n)$ of $Irr(R)$ as the number of irreducible words of length not greater than n.

Corollary 2.3.1. *Let R be the rewriting system and A be the associative k-algebra defined in Theorem 2.3.1. Then the growth γ_A of A is equivalent to the growth $\gamma_{Irr(R)}$ of $Irr(R)$.*

Proposition 2.3.1. *If R is a finite complete rewriting system, then the growth function of $Irr(R)$ is exponential or polynomial.*

Proof. See [Ufn82]. □

Definition 2.3.1. An algebra A is called a *monomial algebra* if it has a presentation such that all the relations are of the form $u = 0$ for a monomial $u \in A$.

Corollary 2.3.2. *Finitely presented monomial algebras have exponential or polynomial growth.*

Proof. It follows from Proposition 2.3.1 and that the fact set of relations of the form $u \to 0$ forms a complete rewriting system for the algebra. □

2.3.1 The Knuth-Bendix Algorithm

We are looking for a procedure to produce a complete rewriting system $\tilde{R}$ for a given rewriting system R such that the algebras associated with R and $\tilde{R}$ as in Theorem 2.3.1 are the same. We refer to [ECH+92] which presents a suitable version of the general *Knuth-Bendix Algorithm* initially appeared in [KB70].

Let X be a finite alphabet, R a finite rewriting system consisting of reductions of the form $u \to v$ for $u, v \in \langle X \rangle$ and $\preccurlyeq$ a semigroup partial ordering on X compatible with R. We construct a sequence of finite sets of reductions R_i, for each $i \geq 0$, by induction. We take $R_0 = R$ and to get R_{i+1} from R_i, we add reductions to make up for failures of the ambiguities. More precisely, for each pair of reductions in R, we check for the following situations: For $A, B, C, P_1, P_2 \in \langle X \rangle$,

(i) *Overlap ambiguity:* If $AB \to P_1$ and $BC \to P_2$, we can reduce ABC in two different ways:

$$\begin{array}{ccc} & ABC & \\ \swarrow & & \searrow \\ P_1C & & AP_2 \end{array}$$

If $P_1C \neq AP_2$, we add either $P_1C \to AP_2$ or $AP_2 \to P_1C$ depending on which word is smaller.

(ii) *Inclusion ambiguity:* If $ABC \to P_1$ and $B \to P_2$, we can reduce ABC in two different ways:

$$\begin{array}{ccc} & ABC & \\ \swarrow & & \searrow \\ P_1 & & AP_2C \end{array}$$

Once again, if $P_1 \neq AP_2C$, we add either $P_1 \to AP_2C$ or $AP_2C \to P_1$.

In rare cases, the procedure stops with a finite set of reductions. Clearly,

$$\langle X \mid u = v,\ u \to v \in R_0 \rangle = \langle X \mid u = v,\ u \to v \in R_i \rangle$$

for all i, because we are adding relations whose sides are already related.

Example 2.3.1. Let $X = \{a, b, c\}$ and $\prec$ be the shortlex order on $\langle X \rangle$ based on the order $a \prec b \prec c$ on X. Let R be a rewriting system consisting of the following reductions

$$\begin{array}{ll} aba \to 0 & acc \to 0 \\ abc \to 0 & b^2a \to ab^2 \\ cba \to 0 & b^2c \to aca \\ cbc \to 0 & \end{array}$$

R is Noetherian and $\prec$ is compatible with R. Take $R = R_0$ and apply the Knuth-Bentix algorithm: The only ambiguity in R_0 whose right hand sides are not equal is

$$\begin{array}{ccc} & b^2acc & \\ \swarrow & & \searrow \\ a^2cac & & 0 \end{array}$$

so, $R_1 = R_0 \cup \{a^2cac \to 0\}$. By repeating the same procedure on R_1, we see that we

have the ambiguity

$$\begin{array}{ccc} & b^2a^2cac & \\ & \swarrow \quad \searrow & \\ a^3ca^2c & & 0 \end{array}$$

and after repeating the same argument n times we get $R_n = R_0 \cup \bigcup_{i=1}^{n} \{a^{i+1}ca^ic \to 0\}$. So $n \to \infty$, we get

$$R_\infty = R_0 \cup \bigcup_{n=1}^{\infty} \{a^{n+1}ca^nc \to 0\}.$$

R_∞ forms a complete rewriting system. In Chapter 3, we will see that the algebra associated with this rewriting system has intermediate growth of type $[e^{\sqrt{n}}]$.

2.4 Lie Algebras and their Universal Enveloping Algebras

A *Lie algebra* over a field k is a vector space with a bilinear operation $[\cdot, \cdot] : L \times L \to L$ satisfying the identities

(i) $[x, x] = 0$,

(ii) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$

for all $x, y, z \in L$. The element $[x, y]$ is called the *Lie bracket* of x and y. (ii) is called the *Jacobi identity*. Bilinearity and (i) together imply the anti-symmetry of the bracket:

(iii) $[x, y] = -[y, x]$ for all $x, y \in L$.

Let M be an associative algebra over k. For all $x, y \in M$, we define

$$[x, y] = xy - yx.$$

This element is called the *commutator* of x and y. Let $[M]$ denote the k-module M with the operation $[x, y] = xy - yx$. It is easily verified that $(x, y) \to [x, y]$ is a

bilinear operation and satisfies the identities (i) and (ii). So $[M]$ with the bracket $[x, y] = xy - yx$ forms a Lie algebra over k. We call $[M]$ the *Lie algebra associated with* M. A k-linear map σ from a Lie algebra L into $[M]$ satisfying

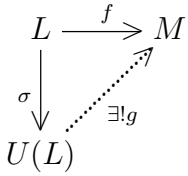
$$\sigma([x, y]) = \sigma(x)\sigma(y) - \sigma(y)\sigma(x) \text{ for } x, y \in L \tag{2.1}$$

is a Lie algebra homomorphism.

Definition 2.4.1. Let L be a Lie algebra over k, TL the tensor algebra of the vector space L over k and I the two sided ideal of TL generated by the tensors $x \otimes y - y \otimes x - [x, y]$ for $x, y \in L$. The associative algebra $U(L) = TL/I$ is called the *universal enveloping algebra* of L. The canonical map of L into $U(L)$ is defined as the restriction to L of the canonical map of TL onto $U(L)$.

The following proposition shows the universal property of $U(L)$.

Proposition 2.4.1. *For any associative algebra M and a Lie algebra homomorphism $f : L \to [M]$ there exists a unique Lie algebra homomorphism $g : [U(L)] \to [M]$ such that $f = g\sigma$ where σ is the canonical map of L into $U(L)$.*



Proof. Let σ' be the canonical map of L into TL then there exists a unique homomorphism g' of TL into M, mapping one-to-one, such that $f = g'\sigma'$. Then, for $x, y \in L$

$$\sigma'(x \otimes y - y \otimes x - [x, y]) = f(x)f(y) - f(y)f(x) - f([x, y])$$

hence $g' = 0$ on I and we can pass to a homomorphism g of $U(L)$ into M such that $f = g\sigma$. The uniqueness of g is immediate since $\sigma(L)$ generates the algebra $U(L)$. □

Proposition 2.4.2. *([Bou89]) Let J be an ideal of a Lie algebra L and σ denote the canonical map of L into $U(L)$. If R is the ideal of $U(L)$ generated by $\sigma(J)$, then*

$$U(L/J) \cong U(L)/R$$

Proof. Let p be the canonical homomorphism of L onto L/J. We need to show that the homomorphism $\tilde{p} : U(L) \to U(L/J)$. defined canonically by p is surjective and its kernel is R. Let $\tilde{\sigma}$ denote the canonical map of L/J into $U(L/J)$. Then the commutative diagram

$$\begin{array}{ccc} L & \xrightarrow{p} & L/J \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\tilde{\sigma}} \\ U(L) & \overset{\tilde{p}}{\dashrightarrow} & U(L/J) \end{array}$$

$\tilde{p} \circ \sigma = \sigma' \circ p$ shows that $\sigma(J) \subseteq Ker(\tilde{\sigma})$, hence $R \subseteq Ker(\tilde{\sigma})$. Let Ψ be the canonical homomorphism of $U(L)$ onto $U(L)/R$. Since $R \subseteq Ker(\tilde{\sigma})$, there exists a homomorphism Φ from $U(L)/R$ into $U(L/J)$.

$$\begin{array}{ccccc} L & \xrightarrow{p} & L/J & & \\ {\scriptstyle\sigma}\downarrow & & \vdots{\scriptstyle\theta} & \searrow^{\tilde{\sigma}} & \\ U(L) & \underset{\Psi}{\rightarrow} & U(L)/R & \underset{\Phi}{\rightarrow} & U(L/J) \end{array}$$

Since $\Psi \circ \sigma(J) = 0$, we define a Lie algebra homomorphism θ of L/J into $U(L)/R$ such that

$$\theta \circ p = \Psi \circ \sigma$$

$$\Phi \circ \theta \circ p = \tilde{\sigma} \circ p = \Phi \circ \Psi \circ \sigma.$$

By the universal property of $U(L/J)$ there exists a unique homomorphism Φ' of $U(L/J)$ into $U(L)/R$ such that

$$\theta = \Phi' \circ \tilde{\sigma}.$$

We get

$$\Phi' \circ \Phi \circ \theta = \Phi' \circ \tilde{\sigma} = \theta$$

and,

$$\Phi \circ \Phi' \circ \tilde{\sigma} = \Phi \circ \theta = \tilde{\sigma}.$$

Hence $\Phi \circ \Phi'$ and $\Phi' \circ \Phi$ are the identity maps of $U(L)/R$ and $U(L/J)$, respectively. And this imply that $U(L/J) \cong U(L)/R$. □

Corollary 2.4.1. *If L is a finitely presented Lie Algebra then its enveloping algebra is also finitely presented.*

2.4.1 Growth of Lie Algebras and Universal Enveloping Algebras

Let k be a field and X a non-empty set. The *free groupoid* $\Gamma(X)$ on X is the set of all non-associative monomials over X. Given $u, v \in \Gamma(X)$, their product is denoted by $[u, v]$. We introduce a free k-module with basis $\Gamma(X)$ and denote it by $F(X)$. For the elements $f = \sum_{u_i \in \Gamma(X)} c_i u_i$ and $g = \sum_{v_i \in \Gamma(X)} c'_i v_i$ of $F(X)$, we set $[f, g] = \sum_{u_i, v_j \in \Gamma(X)} c_i c'_j [u_i, v_j]$ and $F(X)$ becomes a k-algebra with basis $\Gamma(X)$. Let I be the ideal of $F(X)$ generated by the elements of the form $[x, x]$ and $[x, [y, z]] + [y, [z, x]] + [z, [x, y]]$ where $x, y, z \in F(X)$. The *Free Lie algebra with generating set* X is the quotient algebra $\mathcal{F}(X) = F(X)/I$. $F(X)$ has a direct decomposition as $F(X) = \bigoplus_{n=0}^{\infty} F_n(X)$ where $F_n(X)$ is the vector space spanned by monomials of length n in $\Gamma(X)$ and the elements of I are homogenous with respect to this

composition. So $\mathcal{F}(X)$ forms a graded algebra.

$$\mathcal{F}(X) = \bigoplus \mathcal{F}_n(X) \text{ where } \mathcal{F}_n(X) = F_n(X)/(F_n(X) \cap I).$$

An explicit form of a basis of a free Lie algebra (Hall's basis) is given by M. Hall [Hal50]. A.I. Shirshov has given different constructions of bases of free Lie algebras in [Šir58, Šir62].

If $|X| = m \geq 2$ (m is finite) then the growth of the free Lie algebra generated by X is exponential. More precisely, it follows from the classical Witt's formula the dimension of the n^{th} homogeneous component $\mathcal{F}_n(X)$ of $\mathcal{F}(X)$ satisfies:

$$dim_k(F_n(X)) = \frac{1}{n} \sum_{d|n} \mu(d) m^{\frac{n}{d}} \sim \frac{1}{n} m^n$$

where μ is the Möbius function [Bah87].

Let $L = \langle x_1, \ldots, x_m \mid f_1 = 0, \ldots f_r = 0 \rangle$ be a Lie algebra. f_i's are elements of a free Lie algebra i.e., each of them is a linear combination of monomials. Proposition 2.4.2 implies that the associative algebra with identical set of generators and defining relations, where the commutators are thought as in the sense $[x, y] = xy - yx$ is the universal enveloping algebra of L. For instance, the universal enveloping algebra of a free Lie algebra is a free associative algebra, while the universal enveloping algebra of an abelian Lie algebra (i.e., a Lie algebra with zero bracket) is a free commutative algebra. Moreover, knowing a basis of a Lie algebra one can find a basis of its universal enveloping algebra:

Theorem 2.4.1 (Póincare-Birkhoff-Witt Theorem)**.** *If $\{e_1, e_2, \ldots\}$ is a basis of the Lie algebra L, then a basis of $U(L)$ is made up of the products of the form $e_{i_1} e_{i_2} \ldots e_{i_k}$, where $i_1 \leq i_2 \leq \ldots$ and $k \geq 1$.*

Proof. [Ber78b] Given a field k and a Lie algebra L over k with basis $\mathcal{B} = \{e_1, e_2, \ldots\}$, we can form the free associative algebra $k\langle\mathcal{B}\rangle$ generated by $\mathcal{B}$. L can be identified as a free k-submodule of $k\langle\mathcal{B}\rangle$ spanned by $\mathcal{B}$ and the universal enveloping algebra $U(L)$ of L corresponds to the quotient algebra $k\langle\mathcal{B}\rangle/I$ where I is the ideal generated by the elements $xy - yx - [x, y]$ for $x, y \in L$. By the bilinearity and the anti-symmetry of the Lie bracket, the ideal I will be generated by the elements $e_ie_j - e_je_i - [e_i, e_j]$ for $e_i, e_j \in \mathcal{B}$. Let $\leq$ be the shortlex ordering on $\langle\mathcal{B}\rangle$ such that $e_1 < e_2 < \ldots$, and R be the rewriting system on $k\langle\mathcal{B}\rangle$ consisting of the reductions $e_je_i \to e_ie_j - [e_i, e_j]$ for all $e_i, e_j \in \mathcal{B}$ where $i < j$. Then the algebra associated with R is $U(L)$. It can be easily verified that $<$ is a semigroup partial order on $\mathcal{B}$ which is compatible with $\mathcal{B}$ and Noetherian. If we can show that all the ambiguities in R are resolvable then Theorem 2.3.1 implies that the set of irreducible words $Irr(R)$ with respect to R forms a basis for $U(L)$. The ambiguities of R are precisely

$$\begin{array}{ccc} & \nearrow & e_ke_ie_j - e_k[e_i, e_j] = A \\ e_ke_je_i & & \\ & \searrow & e_je_ke_i - [e_j, e_k]e_i = B \end{array}$$

for $i < j < k$ and we have

$$\begin{aligned} e_ke_ie_j &\to e_ie_ke_j - [e_i, e_k]e_j \to e_ie_je_k - e_i[e_j, e_k] - [e_i, e_k]e_j, \\ e_je_ke_i &\to e_je_ie_k - e_j[e_i, e_k] \to e_ie_je_k - [e_i, e_j]e_k - e_j[e_i, e_k]. \end{aligned}$$

So

$$\begin{aligned} A &\to e_ie_je_k - e_i[e_j, e_k] - [e_i, e_k]e_j - e_k[e_i, e_j], \\ B &\to e_ie_je_k - [e_i, e_j]e_k - e_j[e_i, e_k] - [e_j, e_k]e_i. \end{aligned}$$

By Jacobi identity, we have

$$A - B = ([e_i, e_j]e_k - e_k[e_i, e_j]) + (e_j[e_i, e_k] - [e_i, e_k]e_j) + ([e_j, e_k]e_i - e_i[e_j, e_k]) = 0.$$

So all the ambiguities are resolvable with respect to $<$ and

$$Irr(R) = \{e_{i_1}e_{i_2}\dots e_{i_k} \mid i_1 < i_k < \dots < i_k,\ k \geq 1\}$$

forms a basis for $U(L)$. □

Observe that if $L = \bigoplus L_n$ is a graded Lie algebra such that all the components are finite dimensional then its universal enveloping algebra is also graded with the same graduation and by Póincare-Birkhoff-Witt Theorem we have the following relation between the Hilbert series of L and $U(L)$:

Corollary 2.4.2. *If $L = \bigoplus L_n$ is a graded Lie algebra such that all the components are finite dimensional, then*

$$\sum_{n=0}^{\infty} b_n t^n = \prod_{n=1}^{\infty} (1 - t^n)^{-a_n} \tag{2.2}$$

where $a_n := dim_k(L_n)$ and $b_n :=$number of monomials of degree n in $U(L)$.

Proposition 2.4.3. *If a_n and b_n are related by 2.2 and $a_n \sim n^d$ for some $d > 0$, then $b_n \sim e^{n^{\frac{d+1}{d+2}}}$.*

Proof. See for example [Ber83, Pet93, BG00]. □

Corollary 2.4.3. *If a Lie algebra L grows polynomially then its universal enveloping algebra $U(L)$ has intermediate growth. In particular, if L has linear growth then $U(L)$ has growth of type $[e^{\sqrt{n}}]$.*

2.5 Semidirect Product of Lie Algebras

This section is based on first chapter of [Bah87].

Let L be a Lie algebra over a field k. Then a *derivation* of L is a k-linear map $D : L \to L$ such that it obeys the Leibniz rule:

$$D([x, y]) = [Dx, y] + [x, Dy], \text{ for any } x, y \in L.$$

The set of all derivations of L is denoted by $Der_k(L)$. Given $\delta_1, \delta_2 \in Der_k(L)$, $x, y \in L$, we have

$$\begin{aligned}
[\delta_1, \delta_2]([x, y]) &= (\delta_1\delta_2 - \delta_2\delta_1)[x, y] \\
&= \delta_1([\delta_2 x, y] - [x, \delta_2 y]) - \delta_2([\delta_1 x, y] - [x, \delta_1 y]) \\
&= [\delta_1\delta_2 x, y] - [\delta_2 x, \delta_1 y] - [\delta_1 x, \delta_2 y] + [x, \delta_1\delta_2 y] \\
&- [\delta_2\delta_1 x, y] + [\delta_1 x, \delta_2 y] + [\delta_2 x, \delta_1 y] - [x, \delta_2\delta_1 y] \\
&= [\delta_1\delta_2 - \delta_2\delta_1 x, y] + [x, \delta_1\delta_2 - \delta_2\delta_1 y] \\
&= [[\delta_1, \delta_2](x), y] + [x, [\delta_1, \delta_2](y)].
\end{aligned}$$

So $[\delta_1, \delta_2] \in Der_k(L)$. It can be verified that $Der_k(L)$ is a Lie algebra over k. For $x \in L$, let ad_x denote the endomorphism of k-module L whose value on an element $y \in L$ is given by

$$ad_x(y) = [y, x].$$

Since L is a Lie algebra, we have

$$\begin{aligned}
ad_x([y, z]) = [[y, z], x] &= [[y, x], z] + [y, [z, x]] \\
&= [ad_x(y), z] + [y, ad_x(z)].
\end{aligned}$$

So ad_x is a derivation and it is called an *inner derivation* determined by x. The set of all inner derivations of L is denoted by $ad\ L$. There is a natural mapping $ad : L \to Der_k(L)$ that sends $x \in L$ to the inner derivation ad_x determined by x. It is obvious that ad is a homomorphism of k-modules.

Let B and T be Lie algebras over the same field k. Assume that there is given a homomorphism φ of T into the derivation algebra $Der_k(B)$ of B. Let W be the set of all elements of the form $b + t,\ b \in B,\ t \in T$ with scalar multiplication given by

$$\lambda(b + t) = \lambda b + t \text{ for } \lambda \in k.$$

It is clear that W is a k-module. It can be verified that W becomes a Lie algebra if we define the bracket as follows: For $b_1, b_2 \in B,\ t_1, t_2 \in T$,

$$[b_1 + t_1, b_2 + t_2] = [b_1, b_2] + \varphi(t_2)b_1 - \varphi(t_1)b_2 + [t_1, t_2]$$

and W is called the *semidirect product* of B and T corresponding to φ. We denote it by $B \rtimes_\varphi T$. In the case where φ is the zero map, we get the direct product of B by T. If $\varphi(t)$ for any $t \in T$ is the restriction to B of the inner derivation ad_t, then B can be seen as a right T-module and the Lie algebra W is the split extension $B]T$ of B by T.

2.6 Codes and Their Growth

Let $A = \{a_1, \ldots, a_r\}$ be a finite alphabet of cardinality $r \geq 2$. A *formal language* over A is a subset of the set A^* of all words over A. Here, we study a special types of formal languages which are called *(free) codes*. Our exposition borrows from [BP85].

Definition 2.6.1. A nonempty subset X of A^* is called a *(free) code* if for any $n, m \geq 1$ and $x_1, \ldots, x_n, x'_1, \ldots, x'_m \in X,\ x_1 \ldots x_n = x'_1 \ldots x'_m$ implies $n = m$ and

$x_i = x'_i$ for $i \in 1, \ldots, n$ i.e., the monoid $M = \langle X \rangle$ generated by X is free.

Example 2.6.1. For the alphabet $A = \{a, b\}$, $L = \{aa, baa, ba\}$ is a code, but $K = \{a, ab, ba\}$ is not a code since $w = aba \in K^*$ has two different decompositions: $w = aba = (ab)a = a(ba)$.

In general, it is not easy to verify that a given set of words is a code. The book [BP85, I.3] contains a systematic study of the computations required to test that a set of words forms a code. We are interested in various types of codes and examine their asymptotic properties related to different areas of mathematics. Unless otherwise indicated, we assume that codes do not contain the empty word $\emptyset$.

Definition 2.6.2. A subset $K \subset A^*$ is said to be *prefix (resp. suffix)* if no element of K is a prefix (resp. suffix) of another element in K and it is said to be *biprefix* if it is both prefix and suffix.

Lemma 2.6.1. *A prefix (resp. suffix) set different from $\{\emptyset\}$ is a code. Such a code is called a prefix code (resp. suffix code).*

Proof. Let $x_1, \ldots, x_n, x'_1, \ldots, x'_m$ be elements of the prefix set K and let $x_1 \ldots x_n = x'_1 \ldots x'_m$. Assume that i is the smallest number such that $x_i \neq x'_i$ then either x_i is a proper prefix of x'_i or x'_i is a proper prefix of x_i. But this contradicts that K is a prefix set. Similarly, a suffix set forms a code.

□

Let us consider the following properties for $K \subset A^*$:

$(*)$ For any $u \in K$, no proper prefix of u is a suffix of another word $v \in K$.

$(*')$ For any $u \in K$, no prefix of u is a suffix of another word $v \in K$.

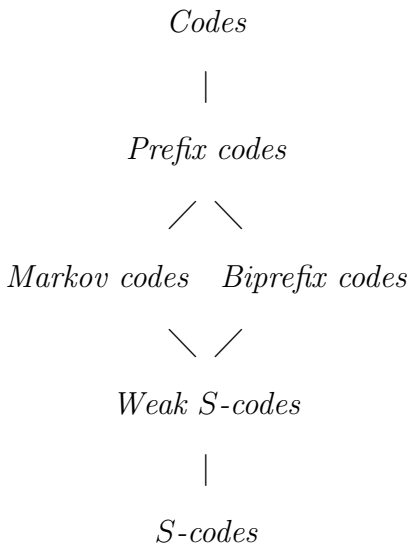
$(**)$ For any $u \in K$, u is not a subword of another word $v \in K$.

Definition 2.6.3. Let K be a subset of A^*

- K is called a *Markov code* if it has property $(*)$.
- K is called a *weak S-code* if it has property $(*')$.
- K is called an *S-code* if it satisfies $(*)$ and $(**)$.

We have the following hierarchy among the different types of codes:

Proposition 2.6.1.



and all the inclusions are strict.

Proof. Note that a set satisfying any of the properties $(*), (*'), (**)$ is a prefix code. It is clear that $(*')$ is a stronger property than $(*)$ and a code satisfying $(*')$ is suffix. Thus weak S-codes are biprefix Markov codes. Since $(*)$ and $(**)$ imply $(*')$, S-codes are weak S-codes. So, the hierarchy among the codes is as given in the above diagram. The code $L = \{abc, bc\}$ forms a Markov code but it is not biprefix (since it is not suffix), so it is not a weak S-code. $T = \{abc, b\}$ is an example of a weak

S-code which is not an S-code. Also, $F = \{a, ab\}$ is a free code which is not a code. So all the inclusions in the diagram are strict. □

The *length* of a word w is defined as the number of letters in it and denoted by $|w|$. A code consisting of words of identical length is called a *block code*. For instance $L = \{a_i b_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s\}$ is a block S-code over an alphabet $A = \{a_1, \ldots, a_r, b_1, \ldots, b_s\}$ where $r, s \geq 1\}$.

Definition 2.6.4. A code (resp. prefix code, Markov code, weak S-code, S-code) X over an alphabet A is called a *maximal* code (resp. prefix code, Markov code, weak S-code, S-code) if X is not properly contained in any other code of the same type over A, that is if $X \subset X'$, where X' is a code (resp. prefix code, Markov code, weak S-code, S-code) over A then $X = X'$.

Example 2.6.2. Let $A = \{a_0, a_1, \ldots, a_{r-1}\}$ be an alphabet where $r \geq 2$. The set $K = \{a_1 \underbrace{a_0 \ldots a_0}_{l_1},\ a_2 \underbrace{a_0 \ldots a_0}_{l_2}, \ldots, a_{r-1} \underbrace{a_0 \ldots a_0}_{l_{r-1}} \mid l_i \geq 0,\ i \in \{1, \ldots, r-1\}\}$ is a maximal S-code. It is called a *canonical code*

Proposition 2.6.2. *Any code (resp. prefix code, Markov code, weak S-code, S-code) over A is contained in some maximal code (resp. prefix code, Markov code, weak S-code, S-code) over A.*

Proof. Follows from Zorn's Lemma. □

Proposition 2.6.3. *Every finite prefix code over a finite alphabet is contained in a maximal finite prefix code.*

Proof. Let L be a finite prefix code over a finite alphabet A and $m = max\{|l| \mid l \in L\}$. Assume that L is not a maximal prefix code and a word $w \in A^*$ is the shortest word such that $L \cup \{w\}$ is a prefix code. If $|w| > m$, then for the prefix w' of w of length

m, $L \cup \{w'\}$ is not a prefix code by the choice of w. This implies that w' has a prefix which is in L , so does w. Hence $|w| \leq m$. Since there are only finitely many elements of length $\leq m$, by adding finitely many words to L, we get a maximal prefix code. $\square$

In view of Proposition 2.6.2 and the hierarchy among the code types given in Proposition 2.6.1, the analogue of Proposition 2.6.3 can be obtained for biprefix codes, Markov codes, weak S-codes and S-codes. But it is not true for codes in general. In [BP85, Example I.5.6], it is shown that any maximal code containing the code $X = \{a^5, ba^2, ab, b\}$ is infinite.

As we defined the growth of finitely generated algebras, we can define the growth of codes. For a finite alphabet A and a code K over A, the following functions:

$$\delta_K(n) = |\{w \in K \mid |w| = n\}|$$

$$\gamma_K(n) = |\{w \in K \mid |w| \leq n\}|$$

are called the *spherical growth function* and *growth function* of K, respectively. It is clear that $1 \leq \delta_K(n) \leq r^n$ for a code K over an alphabet of cardinality r.

The following are the examples of infinite S-codes of different growth types. For $A = \{a_0, \ldots, a_{r-1}\}$, where $r \geq 4$,

- $I = \{a_0 a_1^{n_1} \ldots a_{r-2}^{n_{r-2}} a_{r-1} \mid n_i \in \mathbb{N}\}$ is an S-code with polynomial growth function $\delta_I(n) = \binom{n+r-5}{r-3} \sim n^{r-3}$ for $n \geq 2$.
- $L = \{a_0 w a_{r-1} \mid w \in \{a_1, \ldots, a_{r-2}\}^*\}$ has exponential growth. The spherical growth function of L is $\delta_L(n) = (r-2)^{(n-2)}$ for $n \geq 2$.

- $K = \{a_0 w a_3 \mid w = a_1^{n_1} a_2 a_1^{n_2} a_2 \dots a_2 a_1^{n_k} a_2,\ n_i, k \in \mathbb{N}\}$ forms an S-code over $\{a_0, a_1, a_2, a_3\}$ whose spherical growth function is $\delta_K(n) = p(n-2),\ n \geq 2$ where $p(n)$ is the number of partitions if n. The asymptotic expression for $p(n)$ is given by $\dfrac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}$ as $n \to \infty$ which implies that K has intermediate growth.

The *spherical growth series* F_L and the *growth series* $\tilde{F}_L$ of a code L are defined as $F_L(t) = 1 + \sum_{n=1}^{\infty} \delta_L(n) t^n$ and $\tilde{F}_L(t) = 1 + \sum_{n=1}^{\infty} \gamma_L(n) t^n$, respectively. The relation between $F_L(t)$ and $\tilde{F}_L(t)$ is as follows

$$\tilde{F}_L(t) = (1-t) F_L(t).$$

By Theorem 2.2.1, we know that a code with rational growth series has polynomial or exponential growth.

2.7 Bernoulli Measures and Codes

This section is based on [BP85, I.4]. We give preliminaries about the Bernoulli measures and codes. Later, we will also consider Bernoulli measures on subshifts of the Bernoulli schemes.

A *Bernoulli measure* on A^* is a monoid morphism π from A^* into the multiplicative monoid R_+ of nonnegative real numbers which satisfies $\sum_{a \in A} \pi(a) = 1$ and $\pi(a) > 0$ for all $a \in A$. It follows from the definition that $\pi(\emptyset) = 1$ and $\sum_{u \in A^n} \pi(u) = 1,\ n \geq 1$ where $\emptyset$ is the empty word and A^n denotes the set of words of length n over A . Thus π defines a probability measure on each A^n.

π can be extended to the set of all subsets of A^* by setting for $X \subset A^*$

$$\pi(X) = \sum_{x \in X} \pi(x)$$

Obviously, $\pi(X) \geq 0$ and for any family of $\{X_i\}_{i\in I}$ of subsets of A^*

$$\pi(\bigcup_{i\in I} X_i) \leq \sum_{i\in I} \pi(X_i)$$

and the equality holds if and only if the sets are pairwise disjoint. The value $\pi(X)$ is called the *measure* of the set X with respect to π. If $X, Y \subset A^*$ and

$$XY = \bigcup_{x\in X} \bigcup_{y\in Y} \{xy\}$$

then

$$\pi(XY) \leq \sum_{x\in X} \sum_{y\in Y} \pi(x)\pi(y) = \pi(X)\pi(Y).$$

The following lemma shows that equality holds for codes.

Lemma 2.7.1. *[BP85, Proposition I.4.1] Let L be a code over A and π be a Bernoulli measure on A^* then*

$$\pi(L^n) = \pi(L)^n \text{ for } n \geq 1 \quad \text{and} \quad \pi(L^*) = \sum_{n\geq 0} \pi(L)^n$$

Proof. For $l_1, l_2 \ldots, l_n \in L$, the function $(l_1, l_2, \ldots, l_n) \to l_1 l_2 \ldots l_n$ is a bijection from $\underbrace{L \times L \times \cdots \times L}_{n}$ onto L^n. Thus $\pi(L^n) = \pi(L)^n$ and since $(L^n)_{n\geq 0}$ are pairwise disjoint, $\pi(L^*) = \sum_{n\geq 0} \pi(L^n)$.

□

Theorem 2.7.1. *[BP85, Theorem I.4.2] Let L be a code over A. For any Bernoulli measure π on A^*, $\pi(L) \leq 1$.*

Proof. For a code L, set for $k \geq 1$, $L_k = \{l \in L \mid |l| \leq k\}$. We first prove that $\pi(L_k) \leq 1$ for any k. $L_k \subset A \cup A^2 \cup \cdots \cup A^k$ implies that $(L_k)^n \subset A \cup A^2 \cup \cdots \cup A^{nk}$

for any $n \geq 1$. Thus $\pi((L_k)^n) \leq nk$. If we assume that $\pi(L_k) > 1$, then there exists $\epsilon > 0$ such that $\pi(L_k) = 1 + \epsilon$. With Lemma 2.7.1, this implies

$$\pi((L_k)^n) = (1 + \epsilon)^n$$

and we get $(1 + \epsilon)^n \leq kn$, which is not possible. Hence $\pi(L_k) \leq 1$ and $\pi(L) = \sup_{k \geq 0} \pi(L_k) \leq 1$. □

Corollary 2.7.1. *Let L be a code over A. If there exists a positive Bernoulli measure π on A^* such that $\pi(L) = 1$, then L is a maximal code.*

Corollary 2.7.2. *Let L be a Markov code over an alphabet A such that $L \neq A$. Then for any Bernoulli measure π on A^*, $\pi(L) < 1$.*

Proof. In order to prove this, we show that any Markov code different from the alphabet A is properly contained in a prefix code over A: Let L be a Markov code. If it is a proper subset of A, we are done. So we can assume that there are elements in L of length greater than 1. Let $x \in A$ be the last letter of a word $w \in L$ of length $|w| > 1$. For any $y \in A \backslash \{x\}$, xy overlaps with w, so $xy \notin L$ and there is no word in L whose prefix is xy. Thus $X \cup \{xy\}$ forms a prefix code.
By Proposition 2.6.2 , we conclude that L is properly contained in a maximal code and Corollary 2.7.1 implies that $\pi(L) < 1$. □

The following example shows that Corollary 2.7.2 does not hold for biprefix codes:

Example 2.7.1. Let $A = \{a, b\}$ be an alphabet and $|w|_x$ denote the number of $x \in A$ appears in w. A word w is called a *Dyck word* if $|w|_a = |w|_b$ and $|w'|_a > |w'|_b$ for any proper prefix w' of w. The set D of Dyck words forms a biprefix code. In [BP85, Example I.4.5], it is shown that there exists a Bernoulli measure π on A^* such that $\pi(X) = 1$. By Corollary 2.7.1, this also implies that D is a maximal code.

3. FINITELY PRESENTED QUADRATIC ALGEBRAS OF INTERMEDIATE GROWTH*

3.1 Introduction

The results presented in this section are published in [Koç15]. An algebra defined by quadratic relations is called *quadratic*. The class of quadratic algebras contains a class of finitely presented algebras, called *Koszul algebras* (See [Frö99, BF85a] for the definition). They play an important role in many studies. The main motivation behind the results of this chapter is the following conjecture of A. Polishchuk and L. Positselski [PP05].

Conjecture 1. *The Hilbert series of a Koszul algebra A is a rational function and, in particular, the growth of A is either polynomial or exponential.*

In view of Conjecture 1, we ask the following question:

Question 1. *Are there finitely presented quadratic algebras of intermediate growth?*

The main aim of this chapter is to present examples of finitely presented quadratic algebras of intermediate growth. In order to construct such examples, we first consider the Kac-Moody algebra for the generalized Cartan matrix $\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$. This is a graded Lie algebra of polynomial growth with natural graduation (i.e., generators of the algebra are of degree 1). Next, we consider a suitable subalgebra and its universal enveloping algebra.

*Finitely Presented Quadratic Algebras of Intermediate Growth, by Dilber Koçak, Algebra and Discrete Mathematics, 20(1):69-88, 2015, Copyright ©2015 Lugansk National Taras Shevchenko University. Reprinted with the permission of Lugansk National Taras Shevchenko University.

Theorem 3.1.1. *Let U be the associative algebra with generators x, y and relations $x^3y - 3x^2yx + 3xyx^2 - yx^3 = 0$, $y^3x - 3y^2xy + 3yxy^2 - xy^3 = 0$. Then*

(i) It is the universal enveloping algebra of a subalgebra of the the Kac-Moody algebra for the generalized Cartan matrix $A = \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$.

(ii) U is a graded algebra with generators of degree 1.

(iii) It has intermediate growth of type $e^{\sqrt{n}}$.

(iv) The Veronese subalgebra $V_4(U)$ of U is a quadratic algebra given by 14 *generators and* 96 *quadratic relations and it has the same growth type with U.*

In Section 3.2, we express the Veronese subalgebra of a graded algebra with natural graduation to obtain a finitely presented quadratic algebra of the same growth type. In Section 3.3 we consider a suitable subalgebra of Kac-Moody algebra. We show that it is a finitely presented graded Lie algebra whose generators are of degree 1 and it has linear growth. In Section 3.4 we complete the proof of Theorem 3.1.1 and in Section 3.5 we give another example of a finitely presented associative algebra A of intermediate growth related to the example of the monoid in [Kob95]. A has the following presentation:

$$A = \langle a, b, c \mid b^2a = ab^2,\ b^2c = aca,\ acc = 0,\ aba = 0,\ abc = 0,\ cba = 0,\ cbc = 0 \rangle$$

We show that A has intermediate growth of type $e^{\sqrt{n}}$ and its Veronese subalgebra $V_3(A)$ is an example of finitely presented quadratic algebras of intermediate growth. An explicit presentation of the Veronese subalgebra $V_4(U)$ of the first construction U as an example of a finitely presented quadratic algebra of intermediate growth is given in Appendix.

3.2 The Veronese Subalgebra of an Associative Graded Algebra

Let $A = k\langle x_1, \ldots, x_m\rangle$ be the free associative algebra over a field k with generating set $\{x_1, \ldots, x_m\}$. Each element u of A can be written uniquely as

$$u = u_0 + u_1 + \cdots + u_l,$$

where $A_0 = k$, $u_i \in A_i$ and A_i is the vector space over k spanned by m^i monomials of length i. Let $R = \{f_1, f_2, \ldots, f_s\}$ be a finite set of non-zero homogeneous polynomials with respect to natural gradation (i.e. degrees of all generators are 1) and I be the ideal generated by R. Since I is generated by homogeneous polynomials, the factor algebra $\tilde{A} = A/I$ is graded:

$$\tilde{A} = \tilde{A}_0 \oplus \tilde{A}_1 \oplus \cdots \oplus \tilde{A}_n \oplus \ldots$$

where $\tilde{A}_i = (A_i + I)/I \cong A_i/(A_i \cap I)$. For $d \geq 1$, a *Veronese subalgebra* of $\tilde{A}$ is defined as

$$V_d(\tilde{A}) := k \oplus \tilde{A}_d \oplus \tilde{A}_{2d} \oplus \ldots$$

It is straightforward to see that,

$$growth\ of\ \tilde{A} \sim growth\ of\ V_d(\tilde{A})$$

Proposition 3.2.1. *[BF85b] For sufficiently large d, $V_d(\tilde{A})$ is quadratic.*

Proof. Let $d_1, \ldots, d_s$ be the degrees of $f_1, f_2, \ldots, f_s$ respectively and $d \geq max\{d_i,\ 1 \leq i \leq s\}$. For any two words v', v'' such that

$$deg(v') + d_i + deg(v'') = d$$

consider the element $v'f_iv'' \in A_d$, and for any two words $w',\ w''$ such that

$$deg(w') + d_i + deg(w'') = 2d$$

consider the element $w'f_iw'' \in A_{2d}$. Let $R^* = \{v'f_iv'', w'f_iw''\}$ for $i \in \{1, \ldots, s\}$ and a be a homogeneous element from $V_d(A) \cap I$. Say $a = \sum \alpha v f_i w$, where $\alpha \in k$, v and w are words. Since the degrees of all generators are 1, we can always choose summands v_1, v_2 such that $v = v_1v_2$ and $deg(v_1)$ is a multiple of d, $0 \leq deg(v_2) < d$. Similarly, $w = w_2w_1$, $deg(w_1)$ is a multiple of d, $0 \leq deg(w_2) < d$. Then we will get $deg(v_2f_iw_2) = d$ or $2d$. Hence $v_2f_iw_2 \in R^*$. It shows that $V_d(A) \cap I$ is an ideal generated by the elements of R^* and an element $v'f_iv''$ is a linear combination of free generators of $V_d(A)$ whereas $w'f_iw''$ is a quadratic element in these generators. So $V_d(\tilde{A}) = V_d(A)/(V_d(A) \cap I)$ is a quadratic algebra. □

3.3 An Example of a Finitely Presented Lie Algebra of Linear Growth

The following example is a subalgebra of the Kac-Moody Algebra for the generalized Cartan matrix $A = \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$ [Kac85].

Consider the subalgebra L of $Sl_2(\mathbb{C}[t])$ over $\mathbb{C}$ (i.e., matrices of trace 0 with entries in $\mathbb{C}[t]$) which consists of matrices whose entries on and under the diagonal are divisible by t. That is,

$$L = \{a = (a_{ij})_{2x2} |\ \ a_{ij} \in \mathbb{C}[t],\ tr(a) = 0 \text{ and for } (i,j) \neq (1,2),\ t \text{ divides } a_{ij}\}$$

with the usual Lie bracket $[a, b] = ab - ba$.

Proposition 3.3.1. *Let L be the Lie algebra described above. Then it has the following properties.*

(i) L *is finitely presented with generators* $x := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *and* $y := \begin{pmatrix} 0 & 0 \\ t & 0 \end{pmatrix}$ *and the defining relations* $[x,[x,[x,y]]] = 0$ *and* $[y,[y,[y,x]]] = 0$.

(ii) $L = \bigoplus_{k \geq 1} L_k$ *is graded and generated by* L_1.

(iii) L *has linear growth.*

Proof. Take $x_1 := x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $y_1 := y = \begin{pmatrix} 0 & 0 \\ t & 0 \end{pmatrix}$, and let $z_1 := \begin{pmatrix} t & 0 \\ 0 & -t \end{pmatrix}$. In fact, define $x_i := \begin{pmatrix} 0 & t^{i-1} \\ 0 & 0 \end{pmatrix}$, $y_i := \begin{pmatrix} 0 & 0 \\ t^i & 0 \end{pmatrix}$, and let $z_i := \begin{pmatrix} t^i & 0 \\ 0 & -t^i \end{pmatrix}$ for $i \geq 1$.

An arbitrary element $w \in L$ is of the form:

$$w = \begin{pmatrix} \sum_{i=1}^n m_i t^i & \sum_{i=1}^n k_i t^{i-1} \\ \sum_{i=1}^n l_i t^i & \sum_{i=1}^n -m_i t^i \end{pmatrix} = \sum_{i=1}^n k_i x_i + \sum_{i=1}^n l_i y_i + \sum_{i=1}^n m_i z_i$$

So, any element of L can be written as a linear combination of $x_i,\ y_i,\ z_i$ for $i \geq 1$ and $\{x_i,\ y_i,\ z_i\}_{i=1}^{\infty}$ forms a linearly independent set over $\mathbb{C}$. L has the following relations

$$[x_i, y_j] = z_{i+j-1}, \tag{3.1}$$

$$[x_i, z_j] = -2x_{i+j}, \tag{3.2}$$

$$[y_i, z_j] = 2y_{i+j}, \tag{3.3}$$

$$[x_i, x_j] = 0, \tag{3.4}$$

$$[y_i, y_j] = 0, \tag{3.5}$$

$$[z_i, z_j] = 0. \tag{3.6}$$

for $i, j \geq 1$. In particular,

$$x_{i+1} = -\frac{1}{2}[x_i, z_1],$$

$$y_{i+1} = \frac{1}{2}[y_i, z_1],$$

$$z_i = [x_i, y_1].$$

It follows that L is generated by x_1 and y_1. In order to show that all the relations (3.1) - (3.6) can be derived from the relations $[x_1, [x_1, [x_1, y_1]]] = 0$ and $[y_1, [y_1, [y_1, x_1]]] = 0$, we apply induction on $i + j = n$. If $i + j = 2$, the relations (3.1) - (3.6) hold trivially. If $i + j = 3$,

$$\begin{aligned}
[x_1, y_2] &= [x_1, \tfrac{[y_1, z_1]}{2}] \\
&= -\tfrac{1}{2}\left([z_1, [x_1, y_1]] + [y_1, [z_1, x_1]]\right) \\
&= [x_2, y_1] \\
&= z_2
\end{aligned}$$

$$\begin{aligned}
[x_1, z_2] &= [x_1, [x_2, y_1]] \\
&= -[y_1, [x_1, x_2]] + [x_2, [y_1, x_1]] \\
&= [x_2, [x_1, y_1]] \\
&= [x_2, z_1] \\
&= -2x_3
\end{aligned}$$

$$\begin{aligned}
[y_1, z_2] &= [y_1, [x_1, y_2]] \\
&= -([y_2, [y_1, x_1]] + [x_1, [y_2, y_1]]) \\
&= [y_2, z_1] \\
&= 2y_3
\end{aligned}$$

The relations (3.4)-(3.5) for $n = 3$ correspond to relations of L_0. Observe the following three equations for $[z_2, z_1]$,

$$\begin{aligned}
[z_2, z_1] &= [[x_2, y_1], z_1] \\
&= -([[z_1, x_2], y_1] + [[y_1, z_1], x_2]) \\
&= [[x_2, z_1], y_1] + [x_2, [y_1, z_1]] \\
&= -2[x_3, y_1] + 2[x_2, y_2] \\
&= k
\end{aligned}$$

$$\begin{aligned}
[z_2, z_1] &= [[x_1, y_2], z_1] \\
&= -([[z_1, x_1], y_2] + [[y_2, z_1], x_1]) \\
&= [[x_1, z_1], y_2] + [x_1, [y_2, z_1]] \\
&= -2[x_2, y_2] + 2[x_1, y_3] \\
&= l
\end{aligned}$$

$$\begin{aligned}
[z_2, z_1] &= [z_2, [x_1, y_1] \\
&= -([y_1, [z_2, x_1]] + [x_1, [y_1, z_2]]) \\
&= 2[x_3, y_1] - 2[x_1, y_3] \\
&= m
\end{aligned}$$

3.$[z_2, z_1] = k + l + m = 0$. So, (3.1) - (3.6) hold for $n = 3$. Now, suppose that (3.1) - (3.6) hold for $i + j \leq n$ for some $n \geq 3$. For $1 \leq i \leq n - 1$,

$$\begin{aligned}
[x_i, y_{j+1}] &= \tfrac{1}{2}[x_i, [y_j, z_1]] \\
&= -\tfrac{1}{2}([z_1, [x_i, y_j]] + [y_j, [z_1, x_i]]) \\
&= [x_{i+1}, y_j]
\end{aligned}$$

$$\begin{aligned} -2x_{n+1} &= [x_n, z_1] \\ &= -\tfrac{1}{2}[[x_1, z_{n-1}], z_1] \\ &= \tfrac{1}{2}([[z_1, x_1], z_{n-1}] + [[z_{n-1}, z_1], x_1]) \\ &= [x_2, z_{n-1}] \end{aligned}$$

and,

$$\begin{aligned} [x_i, z_{j+1}] &= [x_i, [x_1, y_{j+1}]] \\ &= -([y_{j+1}, [x_i, x_1]] + [x_1, [y_{j+1}, x_i]]) \\ &= [x_1, z_{i+j}] \end{aligned}$$

Similarly, it can be shown that

$$2y_{n+1} = [y_i, z_{j+1}]$$

for any $i, j \geq 1$ such that $i + j = n$. So (3.1) - (3.3) hold for $i + j = n + 1$.

$$\begin{aligned} [x_1, x_n] &= -\tfrac{1}{2}[x_1, [x_i, z_j]] \\ &= \tfrac{1}{2}([z_j, [x_1, x_i]] + [x_i, [z_j, x_1]]) \\ &= -\tfrac{1}{2}[x_i, [x_1, z_j]] \\ &= [x_i, x_j] \end{aligned}$$

This equality implies $[x_i, x_j] = [x_j, x_i]$. Similarly, one checks that $[y_i, y_j] = [y_j, y_i]$. Hence, (3.4) - (3.5) hold for $i + j = n + 1$.

Finally, we need check that (3.6) holds for $i + j = n + 1$.

$$\begin{aligned} [z_1, z_n] &= [z_1, [x_n, y_1]] &&= 2[x_{n+1}, y_1] - 2[x_n, y_2] \\ &= [z_1, [x_{n-1}, y_2]] &&= 2[x_n, y_2] - 2[x_{n-1}, y_3] \\ &\vdots \\ &= [z_1, [x_1, y_n]] &&= 2[x_2, y_n] - 2[x_1, y_{n+1}] \end{aligned}$$

implies that $n.[z_1, z_n] = 2[x_{n+1}, y_1] - 2[x_1, y_{n+1}]$ and,

$$\begin{aligned} 2[x_1, y_{n+1}] &= [x_1, [y_1, z_n]] &= -[z_n, [x_1, y_1]] - [y_1, [z_n, x_1]] \\ &&= [z_1, z_n] + 2[x_{n+1}, y_1] \end{aligned}$$

So $[z_1, z_n] = 0$. Now, consider $[z_i, z_j]$ for $i \in \{1, \ldots, n-1\}$,

$$\begin{aligned} [z_i, z_j] &= [z_i, [x_j, y_1]] &= -([y_1, [z_i, x_j]] + [x_j, [y_1, z_i]]) \\ &&= 2[x_{i+j}, y_1] - 2[x_j, y_{i+1}] \end{aligned}$$

and,

$$\begin{aligned} [x_j, y_{i+1}] &= \tfrac{1}{2}[x_j, [y_i, z_1] &= -\tfrac{1}{2}([z_1, [x_j, y_i]] + [y_i, [z_1, x_j]]) \\ &&= -\tfrac{1}{2}([z_1, z_n] + [y_i, 2x_{j+1}]) \\ &&= [x_{j+1}, y_i] \end{aligned}$$

By applying this i times we get $[x_j, y_{i+1}] = [x_n, y_1]$, so that

$$[z_i, z_j] = 0 \text{ for } i + j = n + 1$$

i.e., (3.6) holds for $i + j = n + 1$. By (3.1) - (3.3), the set $\{x_i, y_i, z_i\}_{i=1}^{\infty}$ forms a basis for L as a vector space. It can be observed that $L = \bigoplus_{k \geq 1} L_k$ where $L_{2k-1} = \langle x_k \rangle \oplus \langle y_k \rangle$ and $L_k = \langle z_k \rangle$ for $k \geq 1$. Since

$$[L_{2k-1}, L_{2m-1}] \subseteq L_{2(k+m-1)},$$

$$[L_{2k}, L_{2m}] = 0,$$

$$[L_{2k-1}, L_{2m}] \subseteq L_{2(k+m)-1},$$

L admits an $\mathbb{N}$-gradation given by the sum of occurrences of x and y in each commu-

tator i.e., $L = \bigoplus_{k\geq 1} L_k$ is a graded Lie algebra generated by two elements of degree 1 ($deg(a) = min\{n | a \in \bigoplus_{k=1}^{n} L_k)\}$) and L has linear growth ($dim\ L_i \in \{1, 2\}$ for $i \geq 1$).

□

Remark 3.3.1. We notice that L also admits a $\mathbb{Z}$-gradation. It is a 3-graded Lie algebra (in the sense of [dO03]) over $\mathbb{C}$ generated by elements x of degree 1 and y of degree -1 .

3.4 Proof of Theorem 3.1.1

Let $L = \langle x_1, \ldots, x_m \mid f_1 = 0, \ldots, f_r = 0\rangle$ where each of f_i is a linear combination of the commutators (elements of the form $[x_{i_1}, \ldots, x_{i_k}]$ with an arbitrary distribution of parentheses inside). Then the universal enveloping algebra $U(L)$ of L is an associative algebra with the identical set of generators and relations, where the commutators are thought of as in the ordinary associative sense: $[x, y] = xy - yx$ [Bou89, Proposition 2, p.14]. The universal enveloping algebra $U(L) = U$ of $L = \langle x_1, y_1 \mid [x_1, [x_1, [x_1, y_1]]] = 0,\ [y_1, [y_1, [y_1, x_1]]] = 0\rangle$ has the following presentation:

$$U = \langle x_1, y_1 \mid x_1^3y_1 - 3x_1^2y_1x_1 + 3x_1y_1x_1^2 - y_1x_1^3 = 0,\ y_1^3x_1 - 3y_1^2x_1y_1 + 3y_1x_1y_1^2 - x_1y_1^3 = 0\rangle.$$

So, the associative algebra U in Theorem 3.1.1 is the universal enveloping algebra $U(L)$ of L. By Corollary 2.4.3, since L has linear growth, the growth rate of $U(L)$ is intermediate of type $e^{\sqrt{n}}$. In order to obtain a quadratic algebra of intermediate growth we consider a Veronese subalgebra of $V_4(U)$ as explained in the previous section and conclude that for a given finitely presented graded algebra with all generators of degree 1, one can construct a finitely presented graded algebra with all relations of degree 2. $V_4(U)$ is an example of a finitely presented graded algebra with

intermediate growth. It has 14 generators and 96 relations. All these relations can be found in Appendix.

3.5 A Construction Based on Kobayashi's Example

In this section we construct another example of a finitely presented associative algebra with quadratic relations whose growth function is intermediate. For this, we consider the following example of a monoid with 0 that appears in the paper of Kobayashi [Kob95].

$$M = \langle a, b, c \mid ba = ab,\ bc = aca,\ acc = 0 \rangle$$

where $w(a) = w(c) = 1,\ w(b) = 2$, w is a positive weight function on M. Kobayashi shows that M is a finitely presented monoid with solvable word problem which cannot be presented by a regular complete system. In order to prove that it cannot be presented by a regular complete system, he proves that M has intermediate growth. Now, we consider the semigroup algebra $k[M]$ over a field k. $k[M]$ has the same presentation and growth function with M. So $k[M]$ is an example of finitely presented associative graded algebra of intermediate growth. But the generators of $k[M]$ have degrees $deg(a) = deg(c) = 1$ and $deg(b) = 2$. To construct a quadratic algebra with these properties in view of Proposition 3.2.1, we need to consider an algebra whose generators are all of degree 1. Thus we consider the following monoid:

$$\tilde{M} = \langle a, b, c \mid b^2a = ab^2,\ b^2c = aca,\ acc = 0,\ aba = 0,\ abc = 0,\ cba = 0,\ cbc = 0 \rangle$$

where $w(a) = w(b) = w(c) = 1$.

Now, we have the monoid algebra $A := k[\tilde{M}]$ over a field k:

$$A = \langle a, b, c \mid b^2a = ab^2,\ b^2c = aca,\ acc = 0,\ aba = 0,\ abc = 0,\ cba = 0,\ cbc = 0 \rangle$$

where $deg(a) = deg(b) = deg(c) = 1$ To show that A has intermediate growth, we first find a complete rewriting system for A. Let $\prec$ be the shortlex order on $\langle X \rangle$ based on the order $a \prec b \prec c$ i.e.,

$$w_1 \prec w_2 \text{ implies } |w_1| < |w_2| \text{ or } |w_1| = |w_2| \ \&\ w_1 \prec_{lex} w_2.$$

Then A has the rewriting system R consisting of the following relations

$$\begin{aligned} b^2a &\to ab^2 \\ b^2c &\to aca \\ acc &\to 0 \\ aba &\to 0 \\ abc &\to 0 \\ cba &\to 0 \\ cbc &\to 0 \end{aligned}$$

It is easily seen that R is Noetherian. In Example 2.3.1, we have obtained the complete rewriting system $R_\infty = \{b^2a \to ab^2, b^2c \to aca, aba \to 0, abc \to 0, cba \to 0, cbc \to 0, a^nca^{n-1}c \to 0 \mid n \in \mathbb{N}\}$ equivalent to R by applying *Knuth-Bendix Algorithm.*

Since R_∞ is a complete rewriting system, the set of all irreducible words with respect to R_∞, $Irr(R_\infty)$, consists of the words which do not contain u as a subword for any $u \to v \in R_\infty$ and by Theorem 2.3.1, we know that $Irr(R_\infty)$ forms a basis for

A. Words in $Irr(R_\infty)$ are of the following form

$$b^s a^{m_1} c a^{m_2} c \dots a^{m_r} c a^l b^k$$

where $s \in \{0,1\}$, $l,k \in \mathbb{N} \cup \{0\}$ and $0 \leq m_1 \leq m_2 \leq \cdots \leq m_r$, $m_i \in \mathbb{N} \cup \{0\}$ for $i \in \{1, \dots r\}$. So the number of words in $Irr(R^\infty)$ of length n is equal to

$$\sum_{j=0}^{n} (2j+1) \cdot |\{(m_1, \dots, m_r) \mid 0 \leq m_1 \leq \cdots \leq m_r,\ m_1 + \cdots + m_r = n - j - r\}|$$

$$= \sum_{j=0}^{n} (2j+1) \cdot p(n-j)$$

where $p(n)$ is the number of partitions of n. Hence

$$\gamma_A(n) \sim p(n) \sim e^{\sqrt{n}}.$$

A is an example of finitely presented graded algebra with generators of degree 1 and intermediate growth function and its *Veronese subalgebra* $V_3(A)$ can be presented by finitely many quadratic relations (to be precise with 21 generators and 280 relations).

4. ON GROWTH OF FINITELY PRESENTED LIE ALGEBRAS

4.1 Introduction

The examples of finitely presented algebras of intermediate growth in [Ste75, Ufn80] and described in the previous chapter have all growth equivalent to $[e^{\sqrt{n}}]$. This arises the following natural question:

Question 2. *What type of intermediate growth do finitely presented algebras have?*

In this chapter we present examples of finitely presented algebras of intermediate growth greater than $e^{\sqrt{n}}$. Our main result is the following:

Theorem 4.1.1. *For any positive integer d, there exists a finitely presented Lie algebra of polynomial growth $[n^d]$ whose universal enveloping algebra is also finitely presented and has growth $[e^{n^{d/(d+1)}}]$.*

In order to prove the theorem, we consider finitely generated metabelian Lie algebras. In [Bau77], Baumslag established the fact that every finitely generated Lie algebra can be embedded in a finitely presented metabelian Lie algebra which is a homomorphic image of a wreath product of two abelian Lie algebras. We compute the growth of these finitely presented metabelian Lie algebras and show that they are of the type $[e^{n^{d/(d+1)}}]$ for some $d \in \mathbb{N}$.

4.2 Growth of a Finitely Generated Free Metabelian Lie Algebra

Let k be a field and L a Lie algebra over k generated by a finite set X. Elements of X are monomials of length 1. Inductively, a monomial of length n is an element of the form $[u, v]$, where u is a monomial of length $i < n$ and v is monomial of length $n - i$. Every element of L is a linear combination of monomials. If $a_1, \ldots, a_n \in X$

then $[a_1, \ldots, a_n]$ is defined inductively by

$$[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n] \text{ for } n > 2$$

Monomials of the form $[a_1, \ldots, a_n]$ are called *left-normed*. We will frequently use the following simple lemmas in the remainder of this note.

Lemma 4.2.1. *Let $x,\ y,\ z$ be elements of a Lie algebra and $[x, y] = 0$. Then the following relations hold:*

$$[x, [y, z]] = [y, [x, z]]$$

$$[x, z, y] = [y, z, x].$$

Proof. Direct consequence of Jacobi identity. □

Lemma 4.2.2. *Any element of a Lie algebra can be written as a linear combination of left-normed monomials.*

Proof. By induction on the length of monomials. □

Definition 4.2.1. A Lie algebra L is called *solvable of derived length n* if

$$L^{(n)} = 0 \text{ and } L^{(n-1)} \neq 0$$

where $L^{(m+1)} = [L^{(m)}, L^{(m)}]$ and $L^{(0)} = L$. We also denote $L^{(1)} = [L, L]$ by L' and call it the *commutator* of L. A solvable Lie algebra of derived length 2 is called *metabelian*.

Let $X = \{x_1, \ldots, x_d\}$ be a finite set and L_X be the free Lie algebra generated by X. $M = L_X/L_X^{(2)}$ is the free metabelian Lie algebra generated by X. The following proposition can be found in [Bok63].

Proposition 4.2.1. *Let M be a free metabelian Lie algebra over a field k with the generating set $X = \{x_1, \ldots, x_d\}$ and $x_1 < \cdots < x_d$ be an order on X. If $\mathcal{B}$ is the set of left-normed monomials of the form $[a_0, a_1, \ldots, a_{n-1}]$ where $a_0 > a_1 \leq a_2 \leq \cdots \leq a_{n-1}$ for $a_i \in X$ and $n \geq 1$. Then $\mathcal{B}$ forms a basis for M.*

Proof. Let M_n denote the subspace of M spanned by all left-normed monomials of length n in M ($M_0 = k$ and M_1 is the subspace spanned by X). Since the relations $[x, y] = -[y, x]$ for $x, y \in M$ and Jacobi identity are homogeneous, $M_k \cap M_l = \emptyset$ for $k \neq l$. By Lemma 4.2.2, we get $M = \bigoplus_{n=0}^{\infty} M_n$ and $\mathcal{B} = \bigsqcup_{n=1}^{\infty} \mathcal{B}_n$ where $\mathcal{B}_n$ denotes the set of monomials of length n in $\mathcal{B}$. Hence, it is enough to check that $\mathcal{B}_n$ is a basis of M_n for any $n \geq 1$ i.e.,

(i) Any element of M_n can be written as a linear combination of the elements of B_n.

(ii) Elements of $\mathcal{B}_n$ are linearly independent.

For $n = 1$, $\mathcal{B}_1 = X$, so (i) and (ii) hold.

Assume $n = 2$. By the anti-symmetry of the Lie bracket $[x, y] = -[y, x]$ for any $x, y \in X$. So $\mathcal{B}_2$ spans M_2.

Assume $n = 3$ and $y_1, y_2, y_3 \in X$ such that $y_1 \leq y_2 \leq y_3$. There are at most 6 different monomials of length 3 containing y_1, y_2, y_3. They are

$$m_1 = [y_1, y_2, y_3]$$

$$m_2 = [y_1, y_3, y_2]$$

$$m_3 = [y_2, y_1, y_3]$$

$$m_4 = [y_2, y_3, y_1]$$

$$m_5 = [y_3, y_1, y_2]$$

$$m_6 = [y_3, y_2, y_1]$$

m_3 and m_5 are either 0 or the elements of $\mathcal{B}_3$ (For example, if $y_1 = y_3$, $m_5 = 0$).

$$m_1 = [y_1, y_2, y_3] = -[y_2, y_1, y_3] = -m_3$$

$$m_2 = [y_1, y_3, y_2] = -[y_3, y_1, y_2] = -m_5$$

and by Jacobi identity,

$$\begin{aligned} m_4 &= [y_2, y_3, y_1] \\ &= -[y_1, y_2, y_3] - [y_3, y_1, y_2] \\ &= [y_2, y_1, y_3] - [y_3, y_1, y_2] \\ &= m_3 - m_5 \end{aligned}$$

and,

$$m_6 = -m_4 = m_5 - m_3$$

Hence, $\mathcal{B}_3 = \{[x_{i_0}, x_{i_1}, x_{i_2}] \mid x_{i_0} > x_{i_1} \leq x_{i_2},\ x_{i_j} \in X\}$ spans M_3.
Now assume that $\mathcal{B}_k$ spans M_k for any $k \in \{2, 3, \ldots, n\}$. Let $a = [a_0, a_1, \ldots, a_n]$ be an element of length $n+1$ in M where $a_i \in X$. By the assumption $[a_0, a_1, \ldots, a_{n-1}]$ can be written as a linear combination of the elements of $\mathcal{B}_n$. So a is a linear combination of the elements of the form $[a_{i_0}, a_{i_1}, \ldots, a_{i_{n-1}}, a_n]$ where $i_0, i_1, \ldots, i_{n-1}$ is a permutation of $0, 1, \ldots, n-1$ and $a_{i_0} > a_{i_1} \leq \cdots \leq a_{i_{n-1}}$. If $a_n \geq a_i$ for any $i \in \{0, \ldots, n-1\}$, then $[a_{i_0}, a_{i_1}, \ldots, a_{i_{n-1}}, a_n]$ is in $\mathcal{B}_{n+1}$. Otherwise there exists $j \in \{0, \ldots, n-1\}$ such that a_{i_j} is the smallest element satisfying $a_{i_j} > a_n$. If $j = 0$ then again $[a_{i_0}, a_{i_1}, \ldots, a_{i_{n-1}}, a_n]$ is in $\mathcal{B}_{n+1}$. If $j > 0$, we apply Jacobi identity to

$[a_{i_0}, a_{i_1}, \ldots, a_{i_{n-1}}, a_n]$,

$$\begin{aligned}[a_{i_0}, a_{i_1}, \ldots, a_{i_{n-1}}, a_n] &= -[[a_n, [a_{i_0}, \ldots, a_{i_{n-2}}]], a_{n-1}] - [[a_{n-1}, a_n], [a_{i_0}, \ldots, a_{i_{n-2}}]] \\ &= [a_{i_0}, a_{i_1}, \ldots, a_{i_{n-2}}, a_n, a_{n-1}]\end{aligned}$$

For $j \geq 1$, we can repeat this $n - j - 1$ times and get

$$[a_{i_0}, a_{i_1}, \ldots, a_{i_{n-1}}, a_n] = [a_{i_0}, \ldots, a_{i_j}, a_n, a_{i_{j+1}}, \ldots, a_{n-1}] \tag{4.1}$$

If $j \geq 2$, we apply the identity one more time and get

$$[a_{i_0}, a_{i_1}, \ldots, a_{i_{n-1}}, a_n] = [a_{i_0}, \ldots, a_{i_{j-1}}, a_n, a_{i_j}, a_{i_{j+1}}, \ldots, a_{n-1}]$$

and it is a monomial in $\mathcal{B}_{n+1}$. If $j = 1$,

$$[a_{i_0}, a_{i_1}, a_n, a_{i_2}, \ldots, a_{i_{n-1}}]$$

and since $[a_{i_0}, a_{i_1}, a_n]$ is an element of the vector space spanned by $\mathcal{B}_3$, a is a linear combination of monomials in $\mathcal{B}_{n+1}$. To complete the proof , we also need to verify (ii) for any $n \geq 2$:

Since $M_i \cap M_j$ for any i, j, $\sum_{i=1}^{m} c_i p_i(x_1, \ldots, x_d) = 0$ where $c_i \in k$ and $p_i(x_1, \ldots, x_d) \in M_i$ implies that either $k_i = 0$ or $p_i(x_1, \ldots, x_d) = 0$.

If $p_n(x_1, \ldots, x_d) = \sum_{j=1}^{l} c_j [x_{j_1}, \ldots, x_{j_n}]$ for $c_j \in k$, $x_{j_t} \in X$, $j \in \{1, \ldots, l\}$, $t \in \{1, \ldots, n\}$ then the indices $j_1, \ldots, j_n$ are permutations of $1_1, \ldots, 1_n$ for any $j \in \{1, \ldots, l\}$. For $n = 2$, $[x, y] \in \mathcal{B}_2$ implies $[y, x] \notin \mathcal{B}_2$. So $\mathcal{B}_2$ forms a basis for M_2.

For $n = 3$, let $m_1, \ldots, m_6$ be monomials of length 3 as we defined before. Among them only m_3 and m_5 are in $\mathcal{B}_3$, and $m_3 \neq cm_5$ for any $c \in k$. Hence, (ii) holds for

$n = 3$.

Now assume that for $3 \leq i \leq n$, the elements of $\mathcal{B}_i$ are linearly independent and let $[a_0, a_1, \ldots, a_n] \in \mathcal{B}_{n+1}$. Assume that for $i \in \{1, \ldots, m\}$, $m \in \mathbb{N}$, there are indices $i_0, \ldots, i_n$ which are permutations of $0, \ldots, n$ such that

$$[a_{i_0}, \ldots, a_{i_n}] \in \mathcal{B}_{n+1} \text{ for any } i \in \{1, \ldots, m\}$$

and

$$[a_0, a_1, \ldots, a_n] = \sum_{i=1}^{m} c_i [a_{i_0}, \ldots, a_{i_n}] \text{ for some } c_i \in k$$

Choose the smallest element a_j among $\{a_0, \ldots, a_n\}$. It is clear that $j \neq 0$ and if $j = 1$ then there exists $k > 1$ such that $a_1 = a_k$. So we can assume that $j \geq 2$. Similarly, for any $i \in \{1, \ldots, m\}$, there exists $k_i \geq 2$ such that $a_j = a_{i_{k_i}}$. By using equation 4.1, we can replace a_j and a_n in $[a_0, \ldots, a_n]$ and $a_{i_{k_i}}$ and a_{i_n} in all monomials $[a_{i_0}, \ldots, a_{i_n}]$, $i \in \{1, \ldots, m\}$. We get

$$[b, a_j] = \sum_{i=1}^{m} c_i [b_i, a_j]$$

for $b, b_1, \ldots, b_m \in M_n$. Any element of M_n can be written as a linear combination of elements of $\mathcal{B}_n$ but this contradicts that $\mathcal{B}_n$ is linearly independent. Hence, we conclude that $\mathcal{B}$ is a basis of M. □

Corollary 4.2.1. *Let M be a free metabelian Lie algebra over a field k with generating set $X = \{x_1, \ldots, x_d\}$. Then M has polynomial growth of degree d.*

Proof. Let $x_1 < \cdots < x_d$ be the order on X. The growth function of M is

$$\gamma_{X,M}(n) = dim_k(X^n) = \sum_{k=1}^{n} |\mathcal{B}_k|$$

where $\mathcal{B}_k$ denotes the set of basis elements of length k as in Proposition 1. For $m > 2$, consider $\mathcal{B}_m$. The elements of $\mathcal{B}_m$ are of the form $a = [a_0, a_1, \ldots, a_{m-1}]$ where $a_i \in X$ and $a_0 > a_1 \leq a_2 \leq \cdots \leq a_{m-1}$.

If $a_1 = x_j$ for some $j \in 1, \ldots, d-1$ then for $i \in 1, \ldots, m-1$, $a_i \in \{x_j, \ldots, x_d\}$ and $a_0 \in \{x_{j+1}, \ldots, x_d\}$. So for fixed $a_1 = x_j$, the number of basis elements of length m is

$$(d-j)\binom{m-2+d-j}{d-j}$$

Hence,

$$\begin{aligned} |B_m| &= \sum_{j=1}^{d-1}(d-j)\binom{m-2+d-j}{d-j} \\ &= \sum_{j=1}^{d-1}\frac{(m-2+d-1)+\cdots+(m-2+1)}{(d-j-1)!} \\ &\sim \sum_{i=0}^{d-2}\frac{1}{i!}(m-1)^{d-1} \\ &\sim m^{d-1} \end{aligned}$$

Since

$$\gamma_{X,M}(m) = dim_k(X^m) = d + \binom{d}{2} + \sum_{k=3}^{m}|\mathcal{B}_k|,$$

M has polynomial growth of degree d. □

4.3 The Wreath Product of Two Abelian Lie Algebras

Let T and B be Lie algebras over the same field k of characteristic $p \neq 2$. B is a right T-module if there exists a k-bilinear map $B \times T \to B$ satisfying the following :

$$b[t_1, t_2] = (bt_1)t_2 - (bt_2)t_1$$

for $b \in B$, $t_1, t_2 \in T$. As we have seen in Section 2.5, we can describe the semidirect product W of B and T and W is the split extension $B]T$ of B by T. As a vector space $W = B \oplus T$ is the direct sum of B and T, and the Lie operation on W is defined as

$$[b_1 + t_1, b_2 + t_2] = (b_1 t_2 - b_2 t_1) + [t_1, t_2]$$

for $b_1, b_2 \in B$ and $t_1, t_2 \in T$, so W is a Lie algebra over k.

Here, we consider a special case of this construction that can be found in [Bau77, Lic84, Bah87]. Suppose A and T are finite dimensional abelian Lie algebras over a field k of characteristic $p \neq 2$. Let $\{a_1, \ldots, a_m\}$ and $\{t_1, \ldots, t_n\}$ be bases of A and T, respectively. Let $U = U(T)$ be the universal enveloping algebra of T and B be a free right U-module with the module basis $\{a_1, \ldots, a_m\}$. B can be also viewed as a Lie algebra module for T where the action of T on B is the action of a subset of U on the U-module B and hence we can form the split extension $W = B]T$. A and T are Lie subalgebras of W, B is the ideal generated of W generated by $\{a_1, \ldots, a_m\}$ and it is called the *base ideal* of W. W is a Lie algebra generated by A and T. It is termed the *wreath product* of the Lie algebras of A and T and denoted by

$$W = A \wr T$$

(For the general definition of the wreath product of Lie algebras see [Šme73, Bah87]). As a vector space $W = B \oplus T$ is the direct sum of its abelian ideal B and abelian Lie subalgebra T.

Lemma 4.3.1. *[Bau77] Suppose that the Lie algebra W over k is the direct sum of B and T where B is an abelian ideal generated by $\{a_1, \ldots, a_m\}$ and T is an abelian*

Lie algebra generated by $\{t_1, \ldots, t_n\}$*:*

$$W = B \oplus T.$$

Then B *is a Lie algebra spanned by*

$$\{[a_l, t_{j_1}, \ldots, t_{j_s}] \mid \ l \in \{1, \ldots, m\} \text{ and } j_1, \ldots, j_2 \in \{1, 2, \ldots n\}\}.$$

Proof. Firstly, we show that $W = B \oplus T$ is metabelian: Let w, w' be elements of W,

$$w = b + t \text{ and } w' = b' + t', \ \ b, b' \in B \ t, t' \in T.$$

Then,

$$\begin{aligned} [w, w'] &= [b + t, b' + t'] \\ &= [b, b' + t'] + [t, b' + t'] \\ &= [b, b'] + [b, t'] + [t, b'] + [t, t'] \\ &= [b, t'] - [b', t] \in B \end{aligned}$$

this implies that $W' \subset B$. Since B is abelian, $W^{(2)} = 0$. In W, all the elements can be written as linear combinations of left-normed commutators with elements from $\{a_1, \ldots, a_m, t_1, \ldots, t_m\}$. Consider a commutator $x = [x_1, \ldots, x_s]$ for $s \geq 2$ and $x_i \in \{a_1, \ldots, a_m, t_1, \ldots, t_m\}$. If $x \neq 0$ then there is exactly one j such that $x_j \in \{a_1, \ldots, a_m\}$ (In particular $j = 1$ or $j = 2$, otherwise $[x_1, x_2] = 0$): If $x_i \in \{t_1, \ldots, t_n\}$ for all $i \in \{1, \ldots, s\}$, then $x = 0$. If there exist $x_k, x_l \in \{a_1, \ldots, a_m\}$ for some $k \neq l$ then $x = [x_1, \ldots, x_k, \ldots, x_{l-1}, x_l, \ldots x_s] = 0$ since $[x_1, \ldots, x_k, \ldots, x_{l-1}], x_l \in B$ and their product is equal to 0. So W has a basis which is a subset of the following set:

$$\{t_1, \ldots, t_d\} \cup \{[a_l, t_{j_1}, \ldots, t_{j_s}]) \mid \ l \in \{1, \ldots, m\} \text{ and } j_1, \ldots, j_2 \in \{1, 2, \ldots n\}\}.$$

Since $B \cap T = \{0\}$,

$$B \leq span([a_l, t_{j_1}, \ldots, t_{j_s}] \mid \ l \in \{1, \ldots, m\} \text{ and } j_1, \ldots, j_2 \in \{1, 2, \ldots n\})$$

and we have $[a_l, t_{j_1}, \ldots, t_{j_s}] \in B$ for $l \in \{1, \ldots, m\}$ and $j_1, \ldots, j_2 \in \{1, 2, \ldots n\}$. Hence

$$B = span([a_l, t_{j_1}, \ldots, t_{j_s}] \mid \ l \in \{1, \ldots, m\} \text{ and } j_1, \ldots, j_2 \in \{1, 2, \ldots n\}).$$

□

Corollary 4.3.1. *W can be presented by the generators*

$$a_1, \ldots, a_m, t_1, \ldots, t_n$$

and the following relations:

$$[t_i, t_j] = 0$$

for $1 \leq i, j \leq n$,

$$[[a_k, t_{i_1}, \ldots, t_{i_r}], [a_l, t_{j_1}, \ldots, t_{j_s}]] = 0$$

for $1 \leq k, l \leq m,\ \{i_1, \ldots, i_r, j_1, \ldots, j_s\} \subset \{1, 2, \ldots, n\},\ r \geq 0,\ s \geq 0.$

The next lemma follows from a theorem of Lewin [Lew74] and it is reformulated in [Bau77] as:

Lemma 4.3.2. *Let F be a finitely generated free Lie algebra and R an ideal of F. Then there exists a a finite dimensional abelian Lie algebra A such that F/R' can be embedded in $W = A \wr (F/R)$.*

Corollary 4.3.2. *Let M be a finitely generated free metabelian Lie algebra. Then there exist finite-dimensional abelian Lie algebras A and T such that M can be embedded in $W = A \wr T$.*

Proof. Let $R = L'_X$ be the commutator of the free Lie algebra L_X generated by X. Then by Lemma 4.3.2, $M = L_X/L_X^{(2)}$ can be embedded in $W = A \wr T$ where $T = L_X/L'_X$ and A is a finite dimensional abelian Lie algebra. □

4.4 Finitely Presented Metabelian Lie Algebras

Let A and T be finite dimensional abelian Lie algebras over a field k of characteristic $p \neq 2$ and W the wreath product of A and T as we defined in the previous section. In [Bau77], Baumslag showed that W can be embedded in a finitely presented metabelian Lie algebra W^+. The construction of W^+ is as follows:
Let $\{a_1, \ldots a_m\}$ and $\{t_1, \ldots, t_n\}$ be bases of A and T, respectively. Then the universal enveloping algebra U of T is the associative k-algebra $k[t_1, \ldots, t_n]$ of polynomials with variables $t_1, \ldots, t_n$ over k. Furthermore, let B be the free right U-module with module basis $\{a_1, \ldots, a_m\}$. It is well known that U can be turned into a Lie algebra by defining a new multiplication in U by $[u, v] = uv - vu$ U is simply an infinite dimensional abelian Lie algebra and T is a finite dimensional subalgebra of U. To get a finitely presented metabelian Lie algebra W^+, we consider a subalgebra T^+ of the Lie algebra U properly containing T as a subalgebra. Let T^+ be the subalgebra generated by $\{t_1, \ldots, t_n, u_1, \ldots, u_n\}$ where

$$u_i = t_i^2 \text{ for } i \in \{1, \ldots, n\}$$

T^+ is a $2n$-dimensional abelian Lie algebra and we define W^+ as the wreath product of A and T^+ denoted as

$$W^+ = A \wr T^+.$$

Lemma 4.4.1. *[Bau77, Lemma 6] W^+ can be presented on the generators*

$$a_1, \ldots, a_m, t_1, \ldots, t_n, u_1, \ldots, u_n,$$

subject to the relations

$$[[a_k, t_{i_1}, \ldots, t_{i_r}], [a_l, t_{j_1}, \ldots, t_{j_s}]] = 0,$$

$(1 \leq k \leq m,\ 1 \leq l \leq m, i_1, \ldots, i_r, j_1, \ldots, j_r \in \{1, 2, \ldots, n\})$,

$$[t_i, t_j] = [t_i, u_j] = [u_i, u_j] = 0 \quad (1 \leq i \leq n,\ 1 \leq j \leq n),$$

$$[a_k, u_l] = [a_k, t_l, t_l] \quad (1 \leq k \leq n,\ 1 \leq l \leq n).$$

Proof. By the construction of W^+, we have the following relations

$$[a_k, u_i] = a_k t_i^2 = [a_k, t_i, t_i], \tag{4.2}$$

and, since T^+ is abelian

$$[t_i, t_j] = [t_i, u_j] = [u_i, u_j] = 0 \tag{4.3}$$

for any $1 \leq k \leq m,\ 1 \leq i, j \leq n$. It follows from Lemma 4.2.1 and (4.3) that

$$[a_k, x_1, \ldots, x_s] = [a_k, x_{i_1}, \ldots, x_{i_s}] \tag{4.4}$$

if $1 \leq k \leq m$, $x_1, \ldots, x_s \in \{t_1, \ldots, t_n, u_1, \ldots, u_n\}$ and $\{i_1, \ldots, i_s\}$ is any permutation of $1, \ldots, s$. In view of (4.2) and (4.4), we see that

$$[a_k, t_{j_1}, t_{j_2}, \ldots, t_{j_l}, u_i] = [a_k, t_{j_1}, t_{j_2}, \ldots, t_{j_l}, t_i, t_i] \tag{4.5}$$

if $1 \leq k \leq d$, $\{j_1, j_2, \ldots, j_l, i\} \subset \{1, 2, \ldots n\}$. By Lemma 4.3.1 and (4.5), we conclude that all the elements of W^+ can be presented as linear combinations of the monomials of the following set

$$S = \{a_1, \ldots, a_m, t_1, \ldots, t_m, u_1, \ldots, u_m\} \cup \{[a_i, t_{j_1}, \ldots, t_{j_s}] \mid i, j_1, \ldots, j_s \in \{1, \ldots, n\}\}$$

The product of any two elements of S is defined in the given presentation. □

We will use the following lemmas to show that W^+ has a finite presentation.

Lemma 4.4.2. *[Bau77, Lemma 5] Let L be a Lie algebra of characteristic $p \neq 2$. Suppose a, b, t, u are elements of L and suppose*

$$[a, b] = [a, t, b] = [b, t, a] = [t, u] = 0$$

and

$$[a, u] = [a, t, t],\ [b, u] = [b, t, t].$$

Then

$$[[a, \underbrace{t, \ldots, t}_{i}], [b, \underbrace{t, \ldots, t}_{j}]] = 0$$

for every $i \geq 0, j \geq 0$.

Proof. Let us denote $a_0 = a$, $b_0 = b$ and

$$a_i = [a, \underbrace{t, \ldots, t}_{i}],\ b_j = [b, \underbrace{t, \ldots, t}_{j}],\ \text{for } i, j \geq 1.$$

To prove that $[a_i, b_j] = 0$ whenever $i, j \geq 0$, we apply induction on i and j. For $0 \leq i, j \leq 1$,

$$[a_0, b_0] = [a_1, b_0] = [a_0, b_1] = 0$$

are given relations. We only need to verify that $[a_1, b_1] = 0$ to complete the base cases of induction. by Lemma 4.2.1, $[a_1, b_0] = 0$ implies $[a_1, b_1] = [b_0, a_2]$. Similarly, $[b_1, a_0]$ implies $[b_1, a_1] = [a_0, b_2]$. So we get

$$[a_0, b_2] = [a_2, b_0] = [b_1, a_1] \tag{4.6}$$

In view of Lemma 4.2.1 and the given relations $[a_0, u] = a_2$ and $[b_0, u] = b_2$,

$$[a_0, b_2] = [a_0, [b_0, u]] = [b_0, a_2] \tag{4.7}$$

Combining (4.6) and (4.7), we get $[a_0, b_2] = [b_0, a_2] = [a_2, b_0]$. Since $char(k) \neq 2$, we conclude that $[a_0, b_2] = 0$. Thus $[a_1, b_1] = 0$. Now, suppose that

$$[a_i, b_j] = 0 \text{ for } 0 \leq i \leq n,\ 0 \leq j \leq n.$$

Since $[t, u] = 0$, by Lemma 4.2.1, we have

$$[a_i, u] = a_{i+2},\ [b_i, u] = b_{i+2} \text{ for any } i \in \{1, 2, \ldots\}.$$

Combining the induction hypothesis with Lemma 4.2.1 , we get

$$[a_i, b_{n+1}] = [b_n, a_{i+1}] = 0 \text{ for } 0 \leq i \leq n-1 \tag{4.8}$$

and similarly,

$$[b_j, a_{n+1}] = [a_n, b_{j+1}] = 0 \text{ for } 0 \leq j \leq n-1 \tag{4.9}$$

it remains only to verify that

$$[a_n, b_{n+1}] = [a_{n+1}, b_{n+1}] = [b_n, a_{n+1}] = 0.$$

Now $[b_{n-1}, a_{n+1}] = 0$, so by Lemma 4.2.1

$$[b_{n-1}, a_{n+2}] = [b_{n-1}, [a_{n+1}, t]] = [a_{n+1}, b_n] \tag{4.10}$$

and $[b_{n-1}, a_n] = 0$ and $[a_n, b_n] = 0$ imply the following relations, respectively.

$$[b_{n-1}, a_{n+2}] = [b_{n-1}, [a_n, u]] = [a_n, b_{n+1}] \tag{4.11}$$

$$[a_n, b_{n+1}] = [b_n, a_{n+1}] = -[a_{n+1}, b_n] \tag{4.12}$$

Putting (4.10), (4.11) and (4.12) together, we get $-[a_{n+1}, b_n] = [a_{n+1}, b_n]$. Since $char(k) \neq 2$, this implies

$$[a_{n+1}, b_n] = 0 \tag{4.13}$$

and a similar argument shows that

$$[a_n, b_{n+1}] = 0 \tag{4.14}$$

We also need to verify that $[a_{n+1}, b_{n+1}] = 0$. By Lemma 4.2.1 ,

$$[a_n, b_{n+2}] = [b_{n+1}, a_{n+1}] \tag{4.15}$$

$$[a_n, b_{n+2}] = [b_n, a_{n+2}] \tag{4.16}$$

$$[a_{n+1}, b_{n+1}] = [b_n, a_{n+2}] \tag{4.17}$$

Combining (4.15), (4.16) and (4.17), we get

$$[a_{n+1}, b_{n+1}] = [b_{n+2}, a_n] = [a_{n+2}, b_n] = -[a_{n+1}, b_{n_1}]$$

Therefore,

$$[a_{n+1}, b_{n+1}] = 0 \tag{4.18}$$

Equations (4.8), (4.9), (4.13), (4.14) and (4.18) completes the induction and the proof of Lemma 4.4.2. □

Lemma 4.4.3. *For any $k, l \in \{1, 2, \ldots, m\}$ and $i_1, i_2, \ldots, i_s \in \{1, 2, \ldots, n\}$,*

$$[a_k, t_{i_1}, t_{i_2}, \ldots, t_{i_s}, a_l] = 0$$

implies that for any $r \in \{1, \ldots, s-1\}$,

$$[[a_l, t_{i_1}, t_{i_2}, \ldots, t_{i_r}], [a_k, t_{i_{r+1}}, \ldots, t_{i_s}]] = 0.$$

Proof. By Lemma 4.2.1 and equation (4.4) we have

$$
\begin{aligned}
[a_k, t_{i_1}, t_{i_2}, \ldots, t_{i_s}, a_l] &= [a_k, t_{i_2}, t_{i_3}, \ldots, t_{i_s}, t_{i_1}, a_l] \\
&= [[a_l, t_{i_1}][a_k, t_{i_2}, t_{i_3}, \ldots, t_{i_s}] \\
&= [[a_l, t_{i_1}][a_k, t_{i_3}, \ldots, t_{i_s}, t_{i_2}] \\
&= [[a_k, t_{i_3}, \ldots, t_{i_s}], [a_l, t_{i_1}, t_{i_2}] \\
&\ldots \\
&= [[a_l, t_{i_1}, t_{i_2}, \ldots, t_{i_r}], [a_k, t_{i_{r+1}}, \ldots, t_{i_s}]] \\
&= 0.
\end{aligned}
$$

□

Proposition 4.4.1. *W^+ can be presented by the generators*

$$a_1, \ldots, a_m, t_1, \ldots, t_n, u_1, \ldots, u_n,$$

subject to the finitely many relations

$$[a_k, t_{j_1}, t_{j_2}, \ldots, t_{j_s}, a_l] = 0 \quad (k, l \in \{1, 2, \ldots, m\}, 1 \leq j_1 < j_2 < \ldots j_s \leq n),$$

$$[t_i, t_j] = [t_i, u_j] = [u_i, u_j] = 0 \quad (1 \leq i \leq n,\ 1 \leq j \leq n),$$

$$[a_k, u_l] = [a_k, t_l, t_l] \quad (1 \leq k \leq n,\ 1 \leq l \leq n).$$

Proof. By Lemma 4.4.1, we only need to show that

$$[[a_k, t_{i_1}, \ldots, t_{i_r}], [a_l, t_{j_1}, \ldots, t_{j_s}]] = 0, \tag{4.19}$$

where $1 \leq k \leq m,\ 1 \leq l \leq m,\ i_1, \ldots, i_r, j_1, \ldots, j_s \in \{1, 2, \ldots, n\},\ r \geq 0,\ s \geq 0$. To prove this, we apply induction on $r > 0$, $s > 0$:

If $r = s = 1$ we have

$$w = [[a_k, t_{i_1}], [a_l, t_{j_1}]]$$

If $i_1 = j_1$, we can apply Lemma 5 by taking $a = a_k$, $b = a_l$, $t = t_{i_1} = t_{j_1}$, $u = u_{i_1}$. Since we have the relations

$$[a, b] = [a, t, b] = [b, t, a] = [t, u] = 0$$

$$[a, u] = [a, t, t] \text{ and } [b, u] = [b, t, t],$$

we get

$$[[a, t], [b, t]] = 0.$$

If $i_1 \neq j_1$, the equation $w = 0$ follows from Lemma 4.4.3. Now assume that for $r \leq q$, $s \leq q$, we have

$$[[a_k, t_{i_1}, \ldots, t_{i_r}], [a_l, t_{j_1}, \ldots, t_{j_s}]] = 0$$

Consider

$$w = [[a_k, t_{i_1}, \ldots, t_{i_q}, t_{i_{q+1}}], [a_l, t_{j_1}, \ldots, t_{j_s}]]$$

for $s \leq q$. If $t_{i_1}, \ldots, t_{i_q}, t_{i_{q+1}}, t_{j_1}, \ldots, t_{j_s}$ are all distinct, $w = 0$ is followed from one of the given relations and Lemma 4.4.3. If not, we prove $w = 0$ as follows: By Lemma 4.2.1 and equation 4.2.1, we can assume without loss of generality that

$$t_{i_{q+1}} = t_{i_q} = t.$$

Taking $a = [a_k, t_{i_1}, \ldots, t_{i_{q-1}}]$, $b = [a_l, t_{j_1}, \ldots, t_{j_s}]$, $t = t_{i_q}$ and $u = u_{i_q}$, we can apply

Lemma 5. Since a, b, t, u satisfy the relations in Lemma 4.4.2, we have

$$w = [[a_k, t_{i_1}, \ldots, t_{i_q}, t_{i_{q+1}}], [a_l, t_{j_1}, \ldots, t_{j_s}]] = [[a, t, t], b] = 0 \tag{4.20}$$

Similarly, one can show that

$$[[a_k, t_{i_1}, \ldots, t_{i_r}], [a_l, t_{j_1}, \ldots, t_{j_q}, t_{j_{q+1}}]] = 0 \tag{4.21}$$

for $r \leq q$. To complete the proof, we only need to show that

$$[[a_k, t_{i_1}, \ldots, t_{i_q}, t_{i_{q+1}}], [a_l, t_{j_1}, \ldots, t_{j_q}, t_{j_{q+1}}]] = 0$$

and it follows from the equations (4.20), (4.21) and Lemma 4.4.2. □

Remark 4.4.1. In [BG99], R. M. Bryant and J. R. J. Groves give a nice criterion for a finitely generated metabelian Lie algebra to be finitely presented.

4.5 Proof of Theorem 4.1.1

Let W be the wreath product of abelian Lie algebras A and T generated by $\{a_1, \ldots, a_d\}$ and $\{t_1, \ldots, t_d\}$, respectively. In the previous section we have shown that W is a subalgebra of a finitely presented Lie algebra W^+ generated by $\{a_1, \ldots, a_d, t_1, \ldots, t_d, u_1, \ldots, u_d\}$. In order to prove Theorem 1, we compute the growth rate of W^+ in this section. In Corollary 4.3.2, we have shown that the free metabelian Lie algebra M generated by d elements can be embedded in W So we have

$$\gamma_M \sim n^d \precsim \gamma_{W^+}$$

To find an upper bound for the growth rate γ_{W^+} of W^+, we consider the number of the non-zero monomials in W^+. In the proof of Lemma 4.4.1, we have shown that

all the elements of W^+ can be presented as linear combinations of the monomials of the following set

$$S = \{a_i, t_j, u_l \mid i, j, l \in \{1, \ldots, m\}\} \cup \{[a_i, t_{j_1}, \ldots, t_{j_s}] \mid i, j_1, \ldots, j_s \in \{1, \ldots, n\}\}$$

and combining this with equation (4.4) we see that, as a vector space W^+ has a basis which is a subset of the following set:

$$\tilde{S} = \{a_i, t_j, u_l \mid i, j, l \in \{1, \ldots, d\}\} \cup \{[a_i, t_{j_i}, \ldots, t_{j_s}] \mid 1 \leq i \leq d, 1 \leq j_1 \leq \cdots \leq j_s \leq d\}$$

So the growth function $\gamma_{W^+}(n)$ of W^+ is less than or equal to the number of elements of length not greater than n in $\tilde{S}$,

$$\gamma_{W^+}(n) \leq 2d + d + \sum_{s=1}^{n-1} d\binom{s+d-1}{d-1} \sim \sum_{s=1}^{n-1} ds^{d-1} \sim n^d$$

and we conclude that

$$\gamma_{W^+}(n) \sim n^d.$$

By Corollary 2.4.2 and Proposition 2.4.3, we see that the growth of universal enveloping algebra $U(W^+)$ is $e^{n^{d/(d+1)}}$.

$$\gamma_{U(W^+)}(n) \sim e^{n^{d/d+1}}.$$

This completes the proof of Theorem 4.1.1.

5. GROWTH OF CODES AND BERNOULLI MEASURES

5.1 Introduction

In this chapter, we examine the asymptotic properties of different types of codes that we introduced in Section 2.6. The initial motivation for working on codes was their relationship with the isomorphism problem of Bernoulli Schemes which has been worked by many authors [Meš59, BH63, Zas64]. Also, S-codes were considered in another context by Levenshtein [Lev64, Lev70] who called them *completely regular*. We examine codes in terms of growth, exponential growth rate and growth series. In addition, my research includes the relation of codes with Bernoulli schemes. The properties of S-codes covering a Bernoulli scheme were discussed in [Liv74, GS82].

5.2 Examples of Codes

In the rest of this chapter, we frequently use the following examples of finite S-codes that are taken from [Lev70] to build infinite codes with some specific properties. Unless otherwise indicated, all the codes that we define are over the alphabet $A = \{0, 1, \ldots, r-1\}$, $r \geq 2$.

(a) For fixed $k \in \mathbb{N}$, $W_k(n)$, $n > k$, denotes the set of words w of length $|w| = n$ such that w begins with non-zero digit and ends with k zeros; moreover, a word of k zeros does not appear in any proper prefix of w, i.e. w is of the form $w = x\bar{w}y0^k$ where $|w| = n$, $x, y \in \{1, \ldots, r-1\}$, $\bar{w} \in A^*$ such that 0^k is not a subword of $\bar{w}$.

(b) $M(n)$, $n > 1$ consists of all words of length n for which in any proper prefix of length m the number of zeros is not greater than m/r, and in any proper suffix of length m the number of zeros is strictly greater than m/r.

Lemma 5.2.1. *For any $i \geq 1$, any word $w \in M(ri+1)$ contains exactly $i+1$ zeros.*

Proof. Let $|w|_a$, $a \in A$, denote the number of a's in w. It is clear that the first letter of w is different from 0 and the last letter is 0. So

$$w = w'0 = x\bar{w} \text{ for some } \; x \in \{1, \ldots, r-1\} \text{ and } w', \bar{w} \in A^*$$

such that $|w'|_0 \leq i$ and $|\bar{w}|_0 > i$. Hence we get $i < |w|_0 \leq i+1$ which implies that any word $w \in M(ri+1)$ contains exactly $i+1$ zeros. □

The following example is inspired by Markov's example of a prefix code in [Mar70].

(c) Let $K_0 = \{0\}$ and for any $n \in \mathbb{N}$ define recursively

$$K_n = \bigcup_{\substack{j \in \{0, \ldots, n-1\} \\ x_i \in \{1, \ldots, r-1\}}} x_1 \ldots x_{r-1} K_j K_{n-j-1}.$$

Lemma 5.2.2. *K_n satisfies the following properties:*

(i) For $w \in K_n$, $|w| = rn+1$, $|w|_0 = n+1$.

(ii) For $n \geq 1$, $K_n \subset M(rn+1)$. In particular if $|r| = 2$, $K_n = M(2n+1)$

Proof. Both properties can easily be verified by induction on n: $K_0 = \{0\}$ and $K_1 = \{x_1 \ldots x_{r-1}00 \mid \; x_i \in \{1, \ldots, r-1\}\}$. Thus (i) and (ii) hold for $n = 0, 1$. Assume that (i) holds for $l \leq n$ and take $w \in K_{n+1}$. Then for some $x_i \in \{1, \ldots, r-1\}$ and $j \in \{0, \ldots, n\}$, there exist $w_j \in K_j$ and $w_{n-j} \in K_{n-j}$ such that

$$w = x_1 \ldots x_{r-1} w_j w_{n-j} \tag{5.1}$$

So the length of w and the number of zeros in w are

$$|w| = r - 1 + rj + 1 + r(n-j) + 1 = r(n+1) + 1$$

$$|w|_0 = j + 1 + (n-j) + 1 = (n+1) + 1.$$

To show (ii), assume that $K_l = M(rl+1)$ for $l \leq n$. If $w \in K_{n+1}$, then w is of the form (5.1) and it is easy to observe that $w \in M(r(n+1)+1)$. Suppose $r = 2$ and $w \in M(2(n+1)+1)$ then it is of the form $w = 1\bar{w}0$ for some $\bar{w} \in A^*$. $\bar{w}$ is of length $2n+1$ and contains n zeros. If $\bar{w} \in K_n$, then the proof is complete. Suppose $\bar{w} \notin K_n = M(2n+1)$, then there exists $j \in \{1, \ldots, n-1\}$ such that the suffix of $\bar{w}$ of length $2i$ contains i zeros. If we choose the maximum of such j then w can be presented as $w = 1w_{n-j}w_j$ where $w_j \in K_j$ and $w_{n-j} \in K_{n-j}$ which implies that $w \in K_{n+1}$ and this completes the proof of (ii). □

In the rest of this section, we consider the following infinite codes and determine their codes.

- $W_k = \bigcup_{n>k} W_k(n)$
- $M = \bigcup_{i=1}^{\infty} M(ri+1)$, $M_e = \cup_{i=1}^{\infty} M(ri)$ (Note that the subindex e stays for "even" in the case $r = 2$.)
- $V_k = \bigcup_{i=k}^{\infty} \{M(ri) \cap W_k(ri))\}$
- $K = \bigcup_{i=1}^{\infty} K_i$
- $L_s = \{0^{s+1}x0^s y,\ 0^{s+1}xwy0^s z \mid x, y, z \in A \setminus 0,\ 0^s \text{ is not a subword of } w\}$

Proposition 5.2.1. *For fixed k, $r \geq 2$, $W_k = \cup_{n>k} W_k(n)$ is a Markov code which is not a weak S-code over A. Moreover, $\bar{W}_k = W_k \cup \{0\}$ is a maximal Markov code.*

Proof. Since $1w \in W_k(n+1)$ for any $w \in W_k(n)$, W_k is not a suffix code. Assume there are words v and w in W_k such that a proper prefix of w is a suffix of v, i.e., $v = v'u$ and $w = uw'$ for some $v', u, w' \in A^*$ and $w' \neq \emptyset$. The last k digits of v are 0 and the first digit of w is different from 0. So $|u| > k$ and this implies that u contains 0^k as a subword. But it contradicts that u is a proper prefix of w. Hence , W_k is a Markov code. Since all words in W_k start with a non-zero digit, $\bar{W}$ forms a Markov code. Assume it is not a maximal Markov code then there exists a word $w \in A^* \backslash \bar{W}_k$ such that $\bar{W}_k \cup \{w\}$ is a Markov code. It is clear that $w \notin A$ and the first digit of w is different from 0. Observe that any word that begins with non-zero digit and does not contain 0^k as a subword is a proper prefix of a word in W. So, w contains 0^k as a subword, that is, $w = u0^k v$ for $u, v \in A^*$ and u is a word beginning with a non-zero digit and does not contain 0^k as a subword. But the prefix $u0^k$ of w is in $\bar{W}$ and this contradicts that $\bar{W} \cup \{w\}$ is a prefix code.

□

Proposition 5.2.2. *Let* $M = \bigcup_{i=1}^{\infty} M(ri+1)$ *and* $M_e = \bigcup_{i=1}^{\infty} M(ri)$. *Then*

(i) Given a word v *of length* $r-1$ *not containing* 0, $w \in M \cup \{0\}$ *if and only if* $vw \in M_e$.

(ii) M *is a Markov code which is not a weak* S*-code.*

(iii) M_e *is a weak* S*-code but it is not an* S*-code.*

Proof. Let $w \in M \cup \{0\}$ and $v \in \{1, \ldots, r-1\}^*$ such that $|v| = r-1$. If $w = 0$, $v0 \in M(r) \subset M_e$. If $w \in M(ri+1)$ for some $i \geq 1$, the number of zeros in any proper prefix of vw of length m is less than or equal to m/r. Similarly any proper suffix of length $m < |w|$ contains more than m/r zeros. Since $w \in M(ri+1)$ contains exactly $i+1$ zeros, any suffix of vw of length $m > |w|$ contains $i+1$ zeros which is greater

than $(r(i+1)-1)/r \geq m/r$ and $vw \in M(r(i+1)) \subset M_e$. Now consider an element $u \in M_e$ of length ri for some $i \geq 1$. u contains i zeros and the first $r-1$ letters are different from 0 i.e., $u = vw$ for some $v \in \{1, \ldots, r-1\}^*$, $|v| = r-1$. If $i = 1$, $w = 0$. For $i > 1$,

$$|w| = r(i-1)+1 \text{ and } |w|_0 = i$$

since w is a suffix of u, any suffix w' of w contains more that $|w'|/r$ zeros. Let $\bar{w}$ be the prefix of w of length k for some $k \in \{1, \ldots, r(i-1)\}$ then

$$|\bar{w}|_0 \leq i - \frac{(ri-k+1)}{r} \leq \frac{k}{r}.$$

Hence, $w \in M(r(i-1)+1)$ and this completes the proof of (i). For $u, v \in M$, it is clear that no proper prefix of u is a proper suffix of v. To show that M forms a Markov code, we also need to prove that it is a prefix set. Assume that $v, w \in M$ and v is a proper prefix of w. Say $w = vu$ for some $u \in A^*$. There exists $i \in \mathbb{N}$ such that $v \in M(ri+1)$ and v contains exactly $i+1$ zeros. But this contradicts the fact that the number of zeros in any proper prefix of length m is not greater than m/r. So M forms a Markov code. Observe that M is not a suffix code : $1^{r-1}00 \in M(r+1)$ and $1^{r-1}01^{r-1}00 \in M(2r+1)$. Hence it is not a weak S-code.

Similarly, one can show that no proper prefix $u \in M_e$ is a proper suffix of $v \in M_e$. We also need to show that M_e is a biprefix code: Let $v \in M(ri)$ for some $i \geq 2$. By (i), we know that a proper prefix of u of length rj for $j < i$ contains strictly less than j zeros which implies that M_e is a prefix code. By the fact that the elements of $M(ri)$ contains exactly i zeros, we can conclude that M_e is a suffix code. For any $w \in M(ri)$ and $v \in \{1, \ldots, r-1\}^*$ of length $r-1$, $vw0 \in M(r(i+1))$. Hence M_e is a weak S-code but not an S-code.

□

Lemma 5.2.3. *$K = \bigcup_{i=1}^{\infty} K_i$ is a prefix code.*

Proof. By Lemma 5.2.2, we know that $K = M \cup \{0\}$ where M is the Markov code defined in Proposition 5.2.2. Since no word in M begins with 0, K is a prefix code. □

Observe that $\bigcup_{n=2}^{\infty} M(n)$ is not a suffix or prefix code. As $u = 10 \in M(2)$, $v = 100 \in M(3)$ and $w = 1100 \in M(4)$. So u, v, w are all the elements of $\bigcup_{n=2}^{\infty} M(n)$ such that u is a prefix of v and v is a suffix of w. But next proposition shows that it forms a code.

Proposition 5.2.3. *$\bigcup_{n=2}^{\infty} M(n)$ is a code.*

Proof. Assume $w_1, \ldots, w_m, w'_1, \ldots, w'_n \in \cup_{n=2}^{\infty} M(n)$ such that

$$w_1 \ldots w_m = w'_1 \ldots w'_n$$

so w_1 is a prefix of w'_1 or vice versa. Say w_1 is a prefix of w'_1. Then $w_1 = w'_1 v$ for some $v \in A^*$. The number zeros of any suffix v' of v is greater than $|v'|/r$. But v has a suffix v'' which is a prefix of w'_i for some $i \in \{2, \ldots, n\}$ and this contradicts that $w'_i \in M(n)$ for some n. So, $\bigcup_{n=2}^{\infty} M(n)$ is a code.

□

Proposition 5.2.4. *For an integer k, $k \geq 2$, $V_k = \bigcup_{i=k}^{\infty} \{M(ri) \cap W_k(ri)\}$ is an S-code over A.*

Proof. We have shown that $\bigcup_{i=k}^{\infty} M(ri)$ is a weak S-code, so the elements of V_k do not overlap. Assume that there exist $u, u' \in V_k$ such that u' is a subword of u. For some $m, n \in \mathbb{N}_{\geq k}$, $u' \in \{M(rm) \cap W_k(rm)\}$ and $u \in \{M(rn) \cap W_k(rn)\}$. Since u'

is in $W_k(rm)$, the last k letters of it are 0 and by definition of $W_k(n)$, u' can only be the suffix of u. But it contradicts the fact that $\bigcup_{i=k}^{\infty} M(ri)$ is biprefix. So, we conclude that V_k is an S-code.

□

Proposition 5.2.5. *For any $s \in \mathbb{N}$, L_s is a maximal S-code.*

Proof. It is clear that

$$L_s = \{0^{s+1}x0^s y,\ 0^{s+1}xwy0^s z \ \mid\ x, y, z \in A \setminus 0,\ 0^s \text{ is not a subword of } w\}$$

is an S-code. Suppose that there exists $v \in A^* \setminus L_s$ such that $L_s \cup \{v\}$ forms an S-code, i.e., v is a word which is neither a subword of any word in L_s nor overlaps with a word in L_s. v is of the following form

$$v = 0^{i_1}x_1^{j_1} \dots 0^{i_k}x_k^{j_k} \quad \text{where } i_m, j_m \in \mathbb{N},\ x_m \in A \setminus \{0\},\ i_1 \geq s+1.$$

We first verify that $k > 1$: If $k = 1$ then $v = 0^{i_1}x_1^{j_1}$ overlaps with $0^{s+1}x_1^{j_1}0^s 1 \in L_s$. So we get $v = 0^{i_1}x_1^{j_1}\tilde{v}0^{i_k}x_k^{j_k}$ and note that $i_k \in \{1, \dots, s\}$ (otherwise $0^{i_k}x_k^{j_k}$ has a suffix which is a prefix of a word in L_s).

If $\tilde{v}$ does not contain 0^s as a subword then there exists a word in L_s overlapping with v. Hence we conclude that $\tilde{v}$ contains 0^s as a subword. Assume $l \in \{2, \dots, k-1\}$ is the smallest number such that $i_l \geq s$. If $i_l = s$ then $0^{i_1}x_1^{j_1} \dots 0^{i_l}x_l$ (which is a prefix of v) is an element of L_s. Thus $i_l > s$. Let $t|in\{l, \dots, k-1\}$ denote the largest number such that $i_t > s$. Then $0^{i_t}x_t^{j_t} \dots 0^{i_k}x_k^{j_k}$ has a prefix which is in L_s or it is a proper prefix of a word in L_s. Both contradict that $L_s \cup \{v\}$ is an S-code. So, L_s is a maximal S-code.

□

5.3 Growth and Exponential Growth Rate of a Code

The *exponential growth rate* of an infinite code K is

$$\rho = \rho_K = \overline{\lim_{n\to\infty}} \sqrt[n]{\delta_K(n)}$$

where $\delta_K(n)$ is the number of elements in K of length n. For a code K over an alphabet of cardinality r we have $1 \leq \rho_K \leq r$ and K has subexponential growth (i.e., it is strictly less than exponential growth) if and only if $\rho_K = 1$. The following lemma shows that for an S-code K, ρ_K is strictly less than r.

Lemma 5.3.1. *For an alphabet A of cardinality r, the exponential growth rate of an S-code K over A is strictly less than r.*

Proof. Assume that K is an infinite S-code. Take $w \in K$ with $|w| = k$, w is not a subword of any word in $K - \{w\}$. Let $v \in K - \{w\}$ be a word of length $n > k$. There exist $l, m \in \mathbb{N} \cup \{0\}$ such that $n = kl + m$ and $m < k$. Since v does not contain w as a subword, the number of words of length n in K is bounded by

$$\delta_K(n) \leq (r^k - 1)^l r^m + 1 \leq (r^k - 1)^l r^k$$

So,

$$\overline{\lim_{n\to\infty}} \sqrt[n]{\delta_K(n)} \leq \overline{\lim_{l\to\infty}} \sqrt[kl]{(r^k - 1)^l r^k} \leq (r^k - 1)^{1/k} < r.$$

□

This leads to the following questions:

Question 3. *Let Φ_r denote the set of S-codes over A and let $w(r) = \sup_{L\in\phi_r} \rho_L$. Do we have $w(r) = r$?*

Question 4. *Given an alphabet A of cardinality $r \geq 2$, does there exist a weak S-code or a Markov code $K \subset A^*$ with exponential growth rate $\rho_K = r$?*

We are able to answer both questions positively by examining the exponential growth rates of the codes L_s, M and M_e introduced in the previous section.

Theorem 5.3.1. *Let L_s be the S-code over A, $|A| = r$, defined in Section 5.2 and ρ_{L_s} denote the exponential growth rate of L_s then*

$$\lim_{s\to\infty} \rho_{L_s} = r.$$

Proof. Let U_s be the set of words over A not containing 0^s as a subword. Since all the elements of L_s of length greater than $2s+3$ are of the form $0^{s+1}xwy0^sz$ where $w \in U_s$ and $x, y, z \in A \setminus \{0\}$, the growth functions of U_s and L_s are equivalent.
Let a_n denote the number of words of length n in U_s. It can be verified that

$$a_n = \begin{cases} r^n & \text{if } n < s \\ (r-1)(a_{n-1} + a_{n-2} + \cdots + a_{n-s}) & \text{otherwise} \end{cases}$$

Hence, the growth series of U_s is as follows

$$\begin{aligned} F_{U_s}(x) &= \sum_{n=0}^{\infty} a_n x^n &&= \sum_{n=0}^{s-1} r^n x^n + \sum_{n=s}^{\infty} (r-1)(a_{n-1} + a_{n-2} + \cdots + a_{n-s})x^n \\ &&&= \frac{1 + x + \cdots + x^{s-1}}{1 - (r-1)(x + x^2 + \cdots + x^s)} \end{aligned}$$

$F_{U_s}(x)$ has a pole p_s between $1/(r-1)$ and $1/r$. As $s \to \infty$, $p_s \to 1/r$ which implies $\rho_{K_s} \to r$. □

Theorem 5.3.2. *For an alphabet A of cardinality r, there exist a Markov code and a weak S-code with the exponential growth rate equal to r. Namely, M and M_e are*

codes with exponential growth rate r, respectively.

Proof. By the assertion (i) of Proposition 5.2.2, we have the following equality between the spherical growth functions of M and M_e:

$$\delta_{M_e}(ri+r) = (r-1)^{(r-1)}\delta_M(ri+1)$$

Hence the exponential growth rates of M and M_e are equal. To show that $\rho_M = r$, we define a degree function d on A as follows:

$$d(0) = -1 \text{ and } d(i) = \frac{1}{r-1} \text{ for } i \in \{1, \ldots, r-1\}$$

and we extend d to A^* by defining

$$d(w) = \sum_{i=1}^{n} d(x_i) \text{ for any } w = x_1 \ldots x_n,\ x_i \in A.$$

For any word $w \in M(ri+1)$, $i \in \mathbb{N}$ and any proper prefix u of length m, we have

$$\begin{aligned} |u|_0 \leq \frac{m}{r} &\Leftrightarrow \sum_{i=1}^{r-1} |u|_i \geq m - \frac{m}{r} \\ &\Leftrightarrow d(u) \geq \tfrac{-m}{r} + \tfrac{1}{r-1}(m - \tfrac{m}{r}) = 0. \end{aligned}$$

We conclude that for any $w \in M(ri+1)$ is of the form $w = \bar{w}0$ and $\bar{w}$ is a word containing i zeros such that

$$d(\bar{w}) = 0 \text{ and } d(u) \geq 0 \text{ for any prefix } u \text{ of } \bar{w} \tag{5.2}$$

So the cardinality of $M(ri+1)$ is equal to the number of words of length ri satisfying (5.2). To compute this, we use the following combinatorial fact that can be found in

[Sta99]:

Lemma 5.3.2. *Let $B = \{a, b\}$ be the alphabet with $d(a) = -1$, $d(b) = \frac{1}{r-1}$ and $L_i \subset B^*$ be the set of words w such that*

$$|w|_a = i, \quad |w|_b = (r-1)i$$

and for any prefix w' of w, $d(w') \geq 0$ then the number of words in L_i is

$$|L_i| = C_i^r = \frac{1}{ri+1}\binom{ri+1}{i} = \frac{1}{(r-1)i+1}\binom{ri}{i}.$$

C_i^r are known as *r-ary Catalan numbers*. For $r = 2$, C_i^2 correspond to the standard Catalan numbers. There are $r-1$ different numbers of degree $\frac{1}{r-1}$ in A and by Lemma 5.3.2, we conclude that

$$\begin{aligned}\delta_M(ri+1) &= |M(ri+1)| \\ &= (r-1)^{(r-1)i} C_i^r \\ &= (r-1)^{(r-1)i} \frac{1}{(r-1)i+1}\binom{ri}{i}\end{aligned}$$

By Stirling's formula,

$$\sqrt{n}\binom{kn}{n} \geq \frac{k^{k(n-1)+1}}{(k-1)^{(k-1)(n-1)}},$$

$$\delta_M(ri+1) \geq \frac{(r-1)^{(r-1)i}}{((r-1)i+1)\sqrt{i}} \frac{r^{r(i-1)+1}}{(r-1)^{(r-1)(i-1)}} \geq \frac{(r-1)^{(r-1)}}{((r-1)i+1)\sqrt{i}} \frac{r^{ri}}{r^{r-1}} \tag{5.3}$$

and we have

$$\delta_M(ri+1) \leq r^{ri} \tag{5.4}$$

Equations (5.3) and (5.4) imply

$$\rho_{M_e} = \rho_M = \overline{\lim_{n\to\infty}} \sqrt[n]{\delta_M(n)} = r.$$

□

Before concluding this section, we note the following simple fact about the growth functions of S-codes.

Proposition 5.3.1. *For any non negative function $f : \mathbb{N} \to \mathbb{N}$ bounded by an exponential function $g(n) = m^n$ for some $m > 1$, there exist a finite alphabet and an S-code over this alphabet whose growth function is equal to $f(n)$.*

Proof. Assume that $f(n) \leq m^n$ for some $m > 1$ and $A = \{a_1, \ldots, a_r\}$ For sufficiently large r, the number of words of length $n-2$, $n \geq 2$, over A^* is greater than m^n. So we can choose a subset X_n of A^* containing $f(n)$ words of length $n-2$ and denote the union of K_n for $n > 2$ by X,

$$X = \bigcup_{n>2} X_n.$$

By adding new letters $x_1, \ldots, x_{f(1)}, y_1, \ldots, y_{f(2)}, z_1, \ldots, z_{f(2)}$ to A we get the new alphabet $\tilde{A}$ and consider the following code L over $\tilde{A}$:

$$L = \{x_1, \ldots, x_{f(1)}\} \cup \{y_1 z_1, \ldots, y_{f(2)} z_{f(2)}\} \cup \{y_1 w z_1 \mid w \in X\}$$

Since x_i, y_j, z_k are all different for any $i \in \{1, \ldots, f(1)\}$, $j, k \in \{1, \ldots, f(2)\}$ and $w \in K$ does not contain these letters , L forms an S-code and the spherical growth function of L, $\delta_n(L)$, is equal to $f(n)$.

□

5.4 A Construction of a Weak S-code

In this section we construct a family of weak S-codes. For this purpose we first introduce some necessary definitions. The product of words v and w is denoted by vw. The insertion of the word v into the word w is the word w_1vw_2 where w_1 and w_2 are nonempty words with $w_1w_2 = w$. For a code L over an alphabet A, let $\epsilon(L)$ denote the closure of L with respect to the product and insertion operations and $\epsilon^*(L)$ denote the closure of L with respect to insertion. Every element of $\epsilon(L)$ can be written as a product of words $\epsilon^*(L)$. So $\epsilon(L)$ can be seen as a closure of $\epsilon^*(L)$ with respect to multiplication.

In the rest of the section, we assume that K is an S-code over an alphabet A unless otherwise indicated.

Lemma 5.4.1. *Let u, v be words in K and $w \in \epsilon^*(K)$ be the insertion of v into u. Then the only subword of w which is an element of K is v.*

Proof. Let $w = u_1vu_2$ for non empty words u_1, u_2 such that $u = u_1u_2$ and suppose that w contains a subword $x \in K$ other than v. Since $u, v \in K$, x can not be the subword of u_1, u_2 or v. It is a subword of u_1v or vu_2 as shown in the figures.

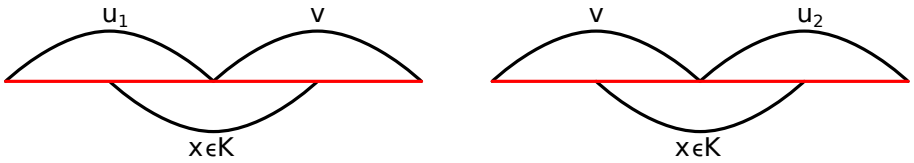


Figure 5.1: The Word x Overlaps with v

So, x and v overlap and it contradicts that K is an S-code. □

We define a sequence $\epsilon_n(K)$, $n \geq 0$, of codes as follows: Let $\epsilon_0(K) = \{\emptyset\}$, $\epsilon_1(K) = K$ and $\epsilon_2(K)$ be the set of words of the form

$$w = v_0 x_1 v_1 \dots x_l v_l \tag{5.5}$$

where $x_1, \dots, x_l \in K$, $v = v_0 \dots v_l \in K$ and, v_0 and v_l are non empty words. $w \in \epsilon_2(K)$ corresponds to the insertion of $x_1, \dots, x_l$ into v.

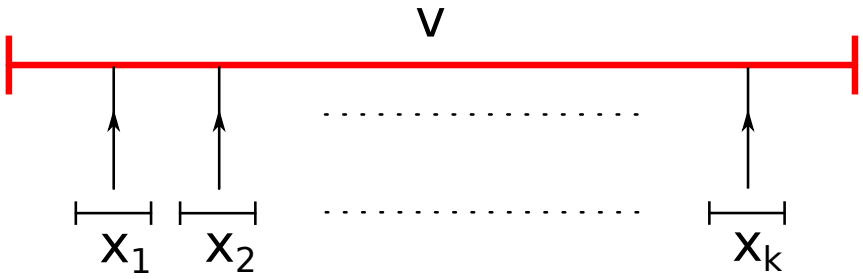


Figure 5.2: The Insertion of $x_1, x_2, \dots, x_k$ into v

By Lemma 5.4.1, w has a unique presentation as in (5.5). For $n \geq 2$, we define $\epsilon_{n+1}(K)$ as the set of words of the form

$$w = v_0 w_1 v_1 \dots w_l v_l \tag{5.6}$$

where $n = max\{m \mid w_i \in \epsilon_m(K),\ i \in \{1, \dots, k\}\}$, $v = v_0 \dots v_l \in K$ and, v_0 and v_l are non empty words.

Lemma 5.4.2. $\epsilon^*(K) = \bigsqcup_{i=1}^{\infty} \epsilon_i(K)$

Proof. It follows from Lemma 5.4.1. □

Theorem 5.4.1. *For an S-code K, $\epsilon^*(K)$ forms a weak S-code.*

Before the proof of Theorem 5.4.1, we first need to state some preliminary results.

Lemma 5.4.3. *If a word $w \in \epsilon^*(K)$ is of the form $w = w'xw''$ where $x \in K$ and $w', w'' \in A^*$, then $w'w'' \in \epsilon^*(K)$.*

Proof. We first note that every word in $\epsilon^*(K)$ contains at least one word of K as a subword. Assume that $w \in \epsilon^*(K)$ is the shortest word such that $w = w'xw''$ for some $x \in K$ and $w'w'' \notin \epsilon^*(K)$. If $w \in \epsilon_l(K)$ for some $l \geq 2$, say

$$w = v_0 w_1 v_1 \dots w_l v_l$$

then there exists $i \in \{1, \dots, l\}$ such that $w_i \in \epsilon_{l-1}(K)$. Let $w_i = w_i' y w_i''$ for some $y \in K$. $|w_i| < |w|$, so $w_i' w_i'' \in \epsilon^*(K)$ or $w_i' w_i''$ is the empty word and this implies

$$\bar{w} = v_0 w_1 v_1 \dots v_{i-1} w_i' w_i'' v_i \dots w_l v_l \in \epsilon^*(K)$$

and this completes the proof if x and y are the same subwords of w. If not, then x and y cannot overlap or one of them can not be the subword of the other. So x is a subword of $\bar{w}$ and the element $\bar{\bar{w}}$ that we get by deleting x from $\bar{w}$ is in $\epsilon^*(K)$. But we can get $w'w''$ by inserting y into $\bar{\bar{w}}$, so $w'w'' \in \epsilon^*(K)$. □

Definition 5.4.1. A word $w \in \epsilon(K)$ is called *indecomposable* if it is not written as a product of more than one words in $\epsilon(K)$.

Lemma 5.4.4. *$\epsilon^*(K)$ is the set of all indecomposable words in $\epsilon(K)$.*

Proof. It is clear that indecomposable elements of $\epsilon(K)$ are in $\epsilon^*(K)$. Assume that $w = w_1 w_2$ is the shortest decomposable element in $\epsilon^*(K)$ where w_1, w_2 are indecomposable words. We know that each word of $\epsilon^*(K)$ contains at least one word of K as a subword which is not prefix or suffix of it. Let $w_1 = w_1' x \bar{w}_1$ for some $x \in K$

and non-empty words $w_1', \bar{w_1} \in A^*$. Then $w_1'\bar{w_1}w_2 \in \epsilon^*(K)$ and this contradicts the assumption that w is the shortest decomposable word in $\epsilon^*(K)$. So w_1 is a word of K. Similarly, $w_2 \in K$. Since $w \notin K$, there exist nonempty words $w', \bar{w} \in A^*$ and a word $y \in K$ such that $w = w'y\bar{w}$.

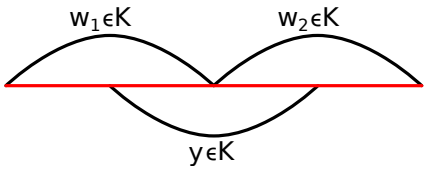


Figure 5.3: The Word y Overlaps with w_1 and w_2

But this contradicts that K is an S-code.

□

Lemma 5.4.5. *$\epsilon^*(K)$ is a biprefix code.*

Proof. Assume that $a \in \epsilon^*(K)$ is the shortest word whose proper prefix b is also in $\epsilon^*(K)$.

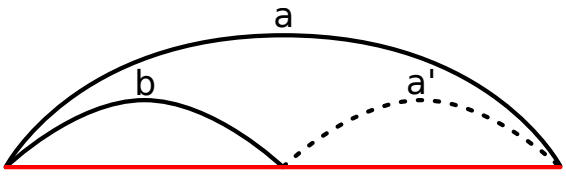


Figure 5.4: The Word b is a Proper Prefix of a

Since a is the shortest one, $b \in K$. By Lemma 5.4.3, we can see that $a' \in \epsilon(K)$.

But it contradicts Lemma 5.4.4. So, $\epsilon^*(K)$ is a prefix code. Similarly, we can show that it is a suffix code. □

Corollary 5.4.1. *Each word $w \in \epsilon(K)$ has a unique decomposition $w = w_1 w_2 \dots w_m$ where $w_i \in \epsilon^*(K)$.*

Proof. All words in $\epsilon(K)$ can be written as a product of the words of $\epsilon^*(K)$ and the uniqueness follows on combining Lemma 5.4.5 with Proposition 2.6.1. □

5.4.1 Proof of Theorem 5.4.1

Proof. By Lemma 5.4.5, it remains only to show that $\epsilon^*(K)$ is a Markov code. Assume that w is the shortest word which contains overlapping words i.e., for $u, v \in \epsilon^*(K)$ there exist u' and v' such that $w = u'v$ and $w = uv'$ where u' and v' are subwords of u and v, respectively.

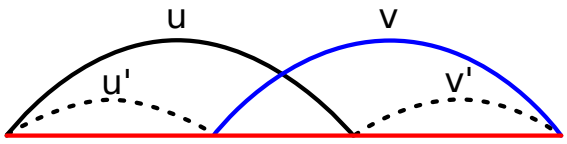


Figure 5.5: Overlapping Words u and v

Since w is the shortest word containing overlapping words as a subword, u' and v' do not contain words of K. So there exists a word $x \in K$ that overlaps with u or v as in one of the following figures:

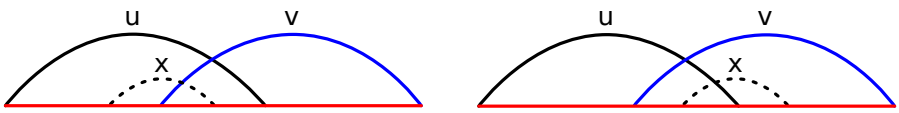


Figure 5.6: The Word x Overlaps with u or v

But all cases contradict that K is an S-code and this completes the proof. □

The following example shows that Theorem 5.4.1 cannot be generalized for an arbitrary code.

Example 5.4.1. $L = \{bde, c, abcd\}$ is a weak S-code over $A = \{a, b, c, d, e\}$. The words $bcde, abcd \in \epsilon^*(L)$ overlap so $\epsilon^*(L)$ is not a weak S-code. Even it is not a Markov code.

Let M_e be the weak S-code defined in Proposition 5.2.2. In the following proposition, we show that it corresponds to a closure of an S-code with respect to insertion.

Proposition 5.4.1. *Let* $T = \{x_1x_2 \dots x_{r-1}0 \mid x_1, \dots, x_{r-1} \in \{1, \dots, r-1\}\}$. M_e *is the closure of the* S*-code with respect to insertion, i.e.,* $\epsilon^*(T) = M_e$.

Proof. It is clear that $T \subset M(r)$ and M_e is closed with respect to insertion, so $\epsilon^*(T) \subset M_e$. In order to show that $M_e = \bigcup_{i=1}^{\infty} M(ri) \subset \epsilon^*(T)$. We apply induction on i: For $i = 1$, the words in $M(r)$ coincide with the words in T. Assume that $\bigcup_{i=1}^{n} M(ri) \subset \epsilon^*(K_r)$ and consider $w \in M(r(n+1))$. The prefix of w of length r does not contain 0 and this implies $w = uxv$ for some non-empty words u and v and a word $x \in K_r$. One can observe that the word $\bar{w} = uv$ is in $M(rn)$, so is in $\epsilon^*(T)$ and this implies $w \in \epsilon^*(T)$.

□

Before ending this section, we note the following results for the growth series of $\epsilon(K)$ and $\epsilon^*(K)$ for an S-code K that will be used later. In [GS82], Grigorchuk and Stepin define the *counting series* of $\epsilon(K)$ and get an equation for this series which we reformulate here for the growth series of $\epsilon(K)$ as follows. And we provide a proof as some details are missing in [GS82].

Theorem 5.4.2. *For an S-code K, the growth series $F_{\epsilon(K)}(t)$ of $\epsilon(K)$ fulfills the following equation*

$$1 - F_{\epsilon(K)}(t) + \sum_{x \in K} t^{|x|}(F_{\epsilon(K)}(t))^{|x|} = 0.$$

Proof. Let v be a word in $\epsilon(K)$. Corollary 5.4.1 implies that v has a unique decomposition as

$$v = w_1 \dots w_k, \;\; w_i \in \epsilon^*(K), \; i \in \{1, \dots, k\}$$

In view of equation (5.5) and Lemma (5.4.2), we define the *rank function* on $\epsilon(K)$ as follows

$$r(v) = r(w_1 \dots w_k) = max\{n \;\mid\; w_i \in \epsilon_n(K), \; i \in \{1, \dots, k\}\}.$$

Let $F(t)$ and $G(t)$ denote the growth series of $\epsilon(K)$ and $\epsilon^*(K)$, respectively. We define the functions $F_n(t)$ and $G_n(t)$:

$$F_n(t) = 1 + \sum_{\substack{v \in \epsilon(K) \\ r(v) \leq n}} t^{|v|} \;\text{ and }\; G_n(t) = 1 + \sum_{\substack{w \in \epsilon^*(K) \\ r(w) \leq n}} t^{|w|}$$

and show that $F_n(t)$ satisfies the following relation

$$F_{n+1}(t) = [1 - \sum_{x \in K} t^{|x|}(F_n(t))^{|x|-1}]^{-1}. \tag{5.7}$$

Let $v \in \epsilon(K)$ be a word of rank not greater than $n+1$. v is a product of elements w of $\bigsqcup_{i=1}^{n+1} \epsilon_i(K)$. If $w \in \epsilon_i(K)$ for $1 \leq i \leq n+1$, then it has a unique presentation as in (5.5):

$$w = v_0 w_1 v_1 \dots w_l v_l$$

where $i = max\{m \mid w_i \in \epsilon_{m-1}(K),\ i \in \{1, \dots, k\}\}$, $v = v_0 \dots v_l \in K$ and, v_0 and v_l are non empty words. So the function $G_{n+1}(t)$ is

$$G_{n+1}(t) = \sum_{x \in K} t^{|x|} (F_n(t))^{|x|-1}$$

and this implies that the growth series of the words of rank not greater than $n+1$ that are products of l elements of $\epsilon^*(K)$ is

$$(\sum_{x \in K} t^{|x|} (F_n(t))^{|w|-1})^l$$

when we take the sum of the series with respect to l, we get equation (5.7). Since the coefficients of t^n is bounded by r^n, $n \in \mathbb{N}$, F_n converges when $t < 1$. Also, the coefficients of the series F_{n+1} is greater than F_n for any n. Hence we take the limit of both sides of equation (5.7) as $n \to \infty$ and get

$$F(t) = (1 - \sum_{x \in K} t^{|x|} (F(t))^{|x|})^{-1}.$$

Hence,

$$1 - F(t) + \sum_{x \in K} t^{|x|} (F(t))^{|x|} = 0.$$

□

Proposition 5.4.2. *The growth series of $\epsilon(K)$ and $\epsilon^*(K)$ for an S-code K satisfy*

the equation

$$F_{\epsilon(K)}(t) = \frac{1}{1 - F_{\epsilon^*(K)}(t)} \tag{5.8}$$

Proof. It follows from Corollary 5.4.1. Since each word $w \in \epsilon(K)$ has a unique decomposition in $\epsilon^*(K)$, we have

$$F_{\epsilon(K)}(t) = \sum_{n=0}^{\infty} (F_{\epsilon^*(K)}(t))^n = \frac{1}{1 - F_{\epsilon^*(K)}(t)}$$

□

Using these results, we provide another solution to Question 4 for the case that the alphabet has even cardinality.

Theorem 5.4.3. *Let $K = \{a_i b_j \mid i, j \in \{1, \ldots, r\}\}$ be the code over the alphabet $A = \{a_i, b_j \mid i, j \in \{1, \ldots, r\}\}$. Then $\epsilon^*(K)$ is a weak S-code with exponential growth rate $2r$.*

Proof. Theorem 5.3.2 implies that $\epsilon^*(K)$ is a weak S-code since K is an S–code. By Theorem 5.4.2, we know that the growth series $F(t)$ of $\epsilon(K)$ satisfies the equation $1 - F(t) + r^2t^2F(t)^2 = 0$. Hence,

$$F(t) = \frac{1 \pm \sqrt{1 - 4r^2t^2}}{2r^2t^2}$$

and by combining this with Proposition 5.4.2 , we get the following relation,

$$F_{\epsilon^*(K)}(t) = 1 - \frac{2r^2t^2}{1 \pm \sqrt{1 - 4r^2t^2}}.$$

We observe that $t = \frac{1}{2r}$ is the smallest positive singular point of $F_{\epsilon^*(K)}(t)$ which implies that the exponential growth rate of $\epsilon^*(K)$ is $2r$. □

5.5 Complete Codes

In this section, we study dense and complete codes. We show that S-codes are never complete and give a sufficient condition for an S-code to be maximal. We refer to the book [BP85] for a comprehensive source regarding the complete codes.

Let X be subset of A^*. An element $w \in A^*$ is called *completable* in X if there exist $u, v \in A^*$ such that $uwv \in X$. A word which is not completable in X is called *incompletable*. X is called *dense* in A^* if all elements of A^* are completable in X. Note that if the cardinality of A is 1, then all the infinite subsets of A^* are dense in A^*.

Theorem 5.5.1. *K is a maximal S-code over an alphabet A if and only if the closure $\epsilon^*(K)$ of K with respect to insertion is dense in A^**

Proof. Assume K is a maximal S-code over A and $w \in A^*$ is the shortest word such that it is not a subword of any word in $\epsilon^*(K)$. Since K is a maximal S-code there exists $v \in K$ such that v and w overlap.

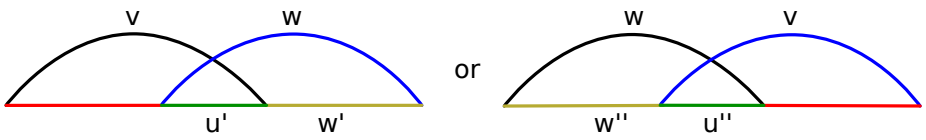


Figure 5.7: The Words v and w Overlap

Since w is the shortest word w' (or w'') is a subword of a word in $\epsilon^*(K)$.

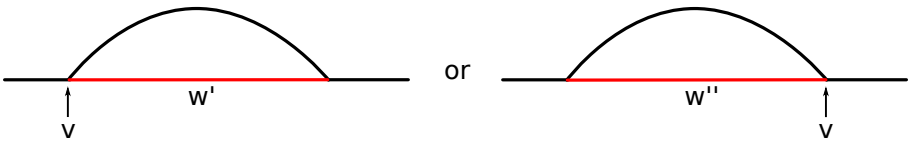


Figure 5.8: The Insertion of v into w' or w''

By inserting v into this word as in the previous figures we get a word in $\epsilon^*(K)$ containing w as a subword.

To prove the sufficiency, assume that K is not a maximal S-code and any word $w \in A^*$ is a subword of an element of $\epsilon^*(K)$. There exists $w \in A^*$ such that $K \cup \{w\}$ is an S-code. Suppose that v is the shortest word in $\epsilon^*(K)$ such that w is a subword of v. We have proven that all the elements of $\epsilon^*(K)$ are of the following forms:

$$v = x_1 v_1 \dots v_n x_n$$

where $x_1 \neq \emptyset$, $x_n \neq \emptyset$, $x_1 \dots x_n \in K$, $v_1, \dots, v_n \in \epsilon^*(K)$.

Since v is the shortest one, w is not a subword of v_i for any $i \in \{1, \dots, n\}$.

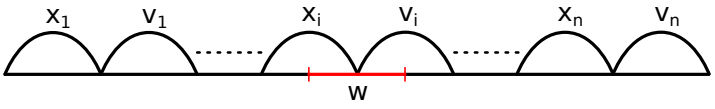


Figure 5.9: A Suffix of w is a Prefix of v_i

or

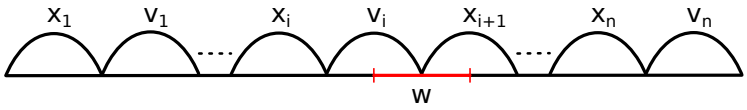


Figure 5.10: A Prefix of w is a Suffix of v_i

We know that every word v_i in $\epsilon^*(K)$ contains a code word as a subword and if we delete it we get another word in $\epsilon^*(K)$ of rank $r(v_i) - 1$. The elements of K can not be a subword of w or can not overlap with w and again by the assumption that v is the shortest word we conclude that $v_i \in K$, but it contradicts that $K \cup \{w\}$ is an S-code. □

Corollary 5.5.1. *The codes M_e and M are dense in A^*.*

Proof. Combining Theorem 5.5.1 and Proposition 5.4.1, we see that M_e is dense in A^*. The correspondence between the elements of M_e and M given in Proposition 5.2.2(i) implies M is also dense. □

Definition 5.5.1. A subset X of A^* is called *complete* if the submonoid X^* generated by X is dense in A^*.

Theorem 5.5.2. *[BP85, Theorem I.5.1] Any maximal code is complete.*

Proof. Let K be a maximal code over A. If $|A| = 1$, any nonempty code is complete, so is K. Assume that $|A| \geq 2$ and K is not complete. Then there exists a word $v \in A^*$ which is incompletable in K^* i.e. $w_1 v w_2 \notin K^*$ for any $w_1, w_2 \in A^*$. Since $|v| = 1$ implies $K \cup \{v\}$ is a code, we can assume that $|v| \geq 2$. Suppose that the first letter of v is a and $b \in A \setminus \{a\}$ and consider the word $\bar{v} = vab^{|v|}$. $\bar{v}$ is a word which does not overlap itself and it is incompletable by the simple fact that any word containing

an incompletable word is also incompletable. To prove the assertion, we will show that $K \cup \{\bar{v}\}$ is a code. If not, then there exist $y_1, \ldots, y_n, y'_1, \ldots, y'_m \in K \cup \{\bar{v}\}$ such that $y_1 \neq y'_1$ and

$$y_1 \ldots y_n = y'_1 \ldots y'_m.$$

Since K is a code, one of $y_1, \ldots, y_n$ is $\bar{v}$ and let i be the smallest such index. $\bar{v}$ is not a subword of any word in K^* implies , one of $y'_1, \ldots, y'_m$ is also $\bar{v}$. Let j is the smallest index such that $y'_j = \bar{v}$. Then we get

$$y_1 \ldots y_{i-1} = y'_1 \ldots y'_{j-1}$$

for $y_1, \ldots, y_{i-1}, y'_1, \ldots, y'_{j-1} \in K$. So $i = j$ and $y_t = y'_t$ for any $t \in \{1, \ldots, i-1\}$ and this contradicts that $y_1 \neq y'_1$. Thus, $K \cup \{\bar{v}\}$ is a code and this completes the proof. □

Following example shows that the inverse of the theorem is not true in general.

Example 5.5.1. By Example 2.7.1, we know that the set D of Dyck words form a maximal free code. For any $u \in A^*$, $v = a^{2|u|_b} u b^{|u|}$ is easily seen to be in D which implies D is dense in A^*. But for each $w \in D$, $D - w$ remains dense, so we get a complete but not a maximal code.

The classification of complete codes is given in the following theorem.

Theorem 5.5.3. *[BP85, Theorem I.5.8] Let L be a code over A. Then L is complete if and only if L is dense or a maximal code.*

The next statement shows that non-trivial S-codes are never complete.

Proposition 5.5.1. *If A is an alphabet and $K \neq A$ is an S-code over A then K is not complete.*

Proof. Let K be an S-code. If K is a proper subset of A, it is clear that K is not complete. So, we can assume that there exists $w = w_1 \dots w_n \in K$ of length $n \geq 2$. Consider the word $w' = ww_n$ and assume there exist $u, v \in A^*$ such that $uw'v \in K^*$, i.e., $uw'v = x_1 \dots x_m$ for some $x_1, \dots, x_m \in K$. There is no word starting with w_n in K, so w overlaps with x_i or it is a subword of x_i for some i. □

Definition 5.5.2. A subset of A^* which is not dense is called *thin*.

Corollary 5.5.2. *If L is a thin Markov code over A, then it is not complete in A^*.*

Proof. It follows from Theorem 5.5.3 and Corollary 2.7.2. □

5.6 A Sufficient Condition for an S-code to be Maximal

Let $A^{\mathbb{Z}} = \prod_{-\infty}^{\infty} A_i$, $A_i = A$ be the infinite product of a countable number of copies of the alphabet A, and let T be the left shift on $A^{\mathbb{Z}}$. For a measure π on A, let μ_π be the product of measures $\pi_i = \pi$ on A_i. The triple $(A^{\mathbb{Z}}, \mu_\pi, T)$ is called a *Bernoulli scheme* where T viewed as a transformation of $(A^{\mathbb{Z}}, \mu_\pi)$ preserving the measure μ_π is called a Bernoulli automorphism.

Every word $w = w_1 w_2 \dots w_r$, for $w_i \in A$, generates a cylindrical set C_w defined as follows

$$C_w = \{\tilde{w} \in A^{\mathbb{Z}} \mid \tilde{w}_i = w_i \, i = 1, 2, \dots, r\}$$

Thus a code $L = \{l_j\}$ itself generates a system of cylindrical sets $\{C_{l_j}\}$. The following theorem appears in [Liv74].

Theorem 5.6.1. *Let natural numbers n_j, $1 \leq j \leq n \leq \infty$, be given not all n_j being equal to 1, and numbers q_j, $0 < q_j < 1$. There exist an alphabet A, an S-code $L = \{l_j\}_{j=1}^m$ over A, and a measure π on A such that*

$$|l_j| = n_j \ , \ \mu_\pi(C_{l_j}) = q_j$$

if and only if for some positive s the series

$$f(t) = 1 - t + \sum q_j t^{n_j}$$

converges on $[0, s]$ *and* $f(s) = 0$.

By using this fact, we can find a bound for the maximum number of words in a block S-code:

Corollary 5.6.1. *Let* $A = \{a_0, a_2, \ldots, a_{r-1}\}$ *be an alphabet of* $r \geq 2$ *letters. The maximum cardinality of an* S*-code whose elements are all of length* r *is* $(r-1)^{r-1}$.

Proof. Consider a distribution with probabilities equal to $p(a_i) = 1/r$ for $a_i \in A$. Let $l = \{l_j\}_1^k$ be an S-code whose elements are all of length d. Then

$$\mu_P(C_{l_j}) = 1/r^r.$$

By Theorem 5.6.1, it is necessary that the polynomial

$$f(t) = 1 - t + (k/r^r)t^r$$

has a positive real root. The greatest among the positive k will be the one for which the polynomial $f(t)$ has a multiple positive real root. This is possible only for $k = (r-1)^{r-1}$. So the maximum number of words in such an S-code is bounded above by $(r-1)^{r-1}$ and we see that this number is attained for the code $K = \{a_0 x_1 \ldots x_{r-1} \mid x_i \in \{a_1, \ldots, a_{r-1},\ i \in \{1, \ldots, r-1\}\}\}$.

□

Definition 5.6.1. For an S-code K and a distribution π on an alphabet A, define

$$\Omega_K = \bigcap_{n=1}^{\infty} \bigcup \{T^s(C_w) \mid w \in \epsilon_j(K),\ j \geq n\ , 1 \leq s \leq |w|\}$$

We say that "S-code K *covers* the scheme $(A^{\mathbb{Z}}, \mu_\pi, T)$" if $\mu_\pi(\Omega_K) = 1$.

The following result of Livshits ([Liv74]) gives the necessary and sufficient condition for an S-code to cover a Bernoulli scheme.

Theorem 5.6.2. *The S-code $K = \{x_i\}_{i=1}^n$, $n \leq \infty$, over an alphabet A covers the Bernoulli scheme $(A^{\mathbb{Z}}, \mu_\pi, T)$ if and only if the series*

$$f(t) = 1 - t + \sum_{i=1}^{n} \mu_\pi(C_{x_i}) t^{|x_i|}$$

has a multiple real positive root in the disk of convergence.

Theorem 5.6.3. *Let $K = \{x_i\}$ be an S-code on the alphabet $A = \{a_1, \ldots, a_d\}$ with probabilities $\pi(a_i) = p_i$. If K covers the Bernoulli scheme $(A^{\mathbb{Z}}, \mu_\pi, T)$ then it is a maximal S-code.*

Proof. Assume that K covers the Bernoulli scheme $(A^{\mathbb{Z}}, \mu_\pi, T)$, then by the previous Theorem,

$$f(t) = 1 - t + \sum_{i=1}^{n} \mu_\pi(C_{x_i}) t^{|x_i|}$$

has a multiple positive real root, say t_o, in the disk of convergence, i.e.,

$$f(t_0) = f'(t_0) = 0$$

One can observe that for $t \in (0, t_0)$, f is decreasing and for $t > t_0$, f is an increasing function. And, since $f(0) = 1$, we conclude that $f(t) \geq 0$ for $t \geq 0$. Now, assume

that there exists $w \in A^* \backslash K$ such that $K_1 = K \cup \{w\}$ is an S-code. The corresponding function for K_1 is

$$f_1(t) = f(t) + \mu_\pi(C_w) t^{|w|}.$$

For $t > 0$, $f_1(t) > f(t) \geq 0$ and this contradicts with Theorem 5.6.1. $\square$

6. SUMMARY

In this dissertation, we have studied the growth of algebras and formal languages. The results that we obtained can be summarized as follows.

In the first part, we have shown the existence of finitely presented quadratic algebras of intermediate growth by giving two concrete examples of such algebras with their presentations.

In the second part, we have focused on finitely presented algebras of different intermediate growth types. By considering the growth of metabelian Lie algebras and their universal enveloping algebras, we have proven the existence of finitely presented algebras of intermediate growth of type $e^{n^{d/(d+1)}}$ for any $d \in \mathbb{N}$.

In the last part, we have studied the growth of formal languages such as S-codes, weak S-codes and Markov codes. It was investigated what type of codes may have maximal growth and given some sufficient conditions for an S-code to be maximal.

REFERENCES

[Bah87] Yu. A. Bahturin. *Identical relations in Lie algebras.* VNU Science Press, b.v., Utrecht, 1987. Translated from the Russian by Bahturin.

[Bas72] H. Bass. The degree of polynomial growth of finitely generated nilpotent groups. *Proc. London Math. Soc. (3)*, 25:603–614, 1972.

[Bau77] Gilbert Baumslag. Subalgebras of finitely presented solvable Lie algebras. *J. Algebra*, 45(2):295–305, 1977.

[Ber78a] George Bergman. A note on growth functions of algebras and semigroups. Unpublished,, 1978.

[Ber78b] George M. Bergman. The diamond lemma for ring theory. *Adv. in Math.*, 29(2):178–218, 1978.

[Ber83] A. E. Bereznyĭ. Discrete subexponential groups. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 123:155–166, 1983. Differential geometry, Lie groups and mechanics, V.

[BF85a] Jörgen Backelin and Ralf Fröberg. Koszul algebras, Veronese subrings and rings with linear resolutions. *Rev. Roumaine Math. Pures Appl.*, 30(2):85–97, 1985.

[BF85b] Jörgen Backelin and Ralf Fröberg. Koszul algebras, Veronese subrings and rings with linear resolutions. *Rev. Roumaine Math. Pures Appl.*, 30(2):85–97, 1985.

[BG99] R. M. Bryant and J. R. J. Groves. Finite presentation of abelian-by-finite-dimensional Lie algebras. *J. London Math. Soc. (2)*, 60(1):45–57, 1999.

[BG00] Laurent Bartholdi and Rostislav I. Grigorchuk. Lie methods in growth of groups and groups of finite width. In *Computational and geometric aspects of modern algebra (Edinburgh, 1998)*, volume 275 of *London Math. Soc. Lecture Note Ser.*, pages 1–27. Cambridge Univ. Press, Cambridge, 2000.

[BH63] J. R. Blum and D. L. Hanson. On the isomorphism problem for Bernoulli schemes. *Bull. Amer. Math. Soc.*, 69:221–223, 1963.

[BK76] Walter Borho and Hanspeter Kraft. Über die Gelfand-Kirillov-Dimension. *Math. Ann.*, 220(1):1–24, 1976.

[Bok63] L. A. Bokut′. A basis for free polynilpotent Lie algebras. *Algebra i Logika Sem.*, 2(4):13–19, 1963.

[Bok76] L. A. Bokut′. Imbeddings into simple associative algebras. *Algebra i Logika*, 15(2):117–142, 245, 1976.

[Bou89] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1989. Translated from the French, Reprint of the 1975 edition.

[BP85] Jean Berstel and Dominique Perrin. *Theory of codes*, volume 117 of *Pure and Applied Mathematics*. Academic Press, Inc., Orlando, FL, 1985.

[dO03] M. P. de Oliveira. On 3-graded Lie algebras in a pair of generators: a classification. *J. Pure Appl. Algebra*, 178(1):73–85, 2003.

[ECH+92] David B. A. Epstein, James W. Cannon, Derek F. Holt, Silvio V. F. Levy, Michael S. Paterson, and William P. Thurston. *Word processing in groups*. Jones and Bartlett Publishers, Boston, MA, 1992.

[Frö99] R. Fröberg. Koszul algebras. In *Advances in commutative ring theory (Fez, 1997)*, volume 205 of *Lecture Notes in Pure and Appl. Math.*, pages 337–350. Dekker, New York, 1999.

[GK66a] I. M. Gel′fand and A. A. Kirillov. On fields connected with the enveloping algebras of Lie algebras. *Dokl. Akad. Nauk SSSR*, 167:503–505, 1966.

[GK66b] I. M. Gelfand and A. A. Kirillov. Sur les corps liés aux algèbres enveloppantes des algèbres de Lie. *Inst. Hautes Études Sci. Publ. Math.*, (31):5–19, 1966.

[Gov72] V. E. Govorov. Graded algebras. *Mat. Zametki*, 12:197–204, 1972.

[Gri83] R. I. Grigorchuk. On the Milnor problem of group growth. *Dokl. Akad. Nauk SSSR*, 271(1):30–33, 1983.

[Gri84] R. I. Grigorchuk. Construction of p-groups of intermediate growth that have a continuum of factor-groups. *Algebra i Logika*, 23(4):383–394, 478, 1984.

[Gro81] Mikhael Gromov. Groups of polynomial growth and expanding maps. *Inst. Hautes Études Sci. Publ. Math.*, (53):53–73, 1981.

[GS82] R. I. Grigorchuk and A. M. Stëpin. On coding of Markov sources. In *Ergodic theory and related topics (Vitte, 1981)*, volume 12 of *Math. Res.*, pages 207–229. Akademie-Verlag, Berlin, 1982.

[Gui70] Yves Guivarc'h. Groupes de Lie à croissance polynomiale. *C. R. Acad. Sci. Paris Sér. A-B*, 271:A237–A239, 1970.

[Hal50] Marshall Hall, Jr. A basis for free Lie rings and higher commutators in free groups. *Proc. Amer. Math. Soc.*, 1:575–581, 1950.

[Kac85] V.G. Kac. *Infinite Dimensional Lie Algebras.* Cambridge University Press, 1985.

[KB70] Donald E. Knuth and Peter B. Bendix. Simple word problems in universal algebras. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 263–297. Pergamon, Oxford, 1970.

[KKM83] A. A. Kirillov, M. L. Kontsevich, and A. I. Molev. Algebras of intermediate growth. *Akad. Nauk SSSR Inst. Prikl. Mat. Preprint*, (39):19, 1983. Translated in Selecta Math. Soviet. **9** (1990), no. 2, 137–153.

[KL00] G.R. Krause and T.H. Lenagan. *Growth of Algebras and Gelfand-Kirillov Dimension.* Graduate Studies in Mathematics. American Mathematical Society, 2000.

[Kob95] Yuji Kobayashi. A finitely presented monoid which has solvable word problem but has no regular complete presentation. *Theoret. Comput. Sci.*, 146(1-2):321–329, 1995.

[Koç15] Dilber Koçak. Finitely presented quadratic algebras of intermediate growth. *Algebra and Discrete Mathematics*, 20(1):69–88, 2015.

[Lev64] V. I. Levenšteĭn. Decoding automata which are invariant with respect to the initial state. *Problemy Kibernet. No.*, 12:125–136, 1964.

[Lev70] V. N. Levenšteĭn. The maximal number of words in codes without overlap. *Problemy Peredači Informacii*, 6(4):88–90, 1970.

[Lew74] Jacques Lewin. A matrix representation for associative algebras. I, II. *Trans. Amer. Math. Soc.*, 188:293–308; ibid. 188 (1974), 309–317, 1974.

[Lic84] A. I. Lichtman. Growth in enveloping algebras. *Israel J. Math.*, 47(4):296–304, 1984.

[Liv74] A. N. Livshits. On the isomorphism problem for Bernoulli schemes. *Teor. Veroyatnost. i Primenen.*, 19(2):409–416, 1974.

[LM01] Alla A. Lavrik-Männlin. On some semigroups of intermediate growth. *Internat. J. Algebra Comput.*, 11(5):565–580, 2001.

[LU95] A. I. Lichtman and V. A. Ufnarovski. On growth of Lie algebras. *Algebra Colloq.*, 2(1):45–49, 1995.

[Mar70] Al. A. Markov. Certain properties of infinite prefix codes. *Problemy Peredači Informacii*, 6(1):97–98, 1970.

[Meš59] L. D. Mešalkin. A case of isomorphism of Bernoulli schemes. *Dokl. Akad. Nauk SSSR*, 128:41–44, 1959.

[Mil68a] J. Milnor. A note on curvature and fundamental group. *J. Differential Geometry*, 2:1–7, 1968.

[Mil68b] John Milnor. Growth of finitely generated solvable groups. *J. Differential Geometry*, 2:447–449, 1968.

[Pet93] V. M. Petrogradskiĭ. Some type of intermediate growth in Lie algebras. *Uspekhi Mat. Nauk*, 48(5(293)):181–182, 1993.

[PP05] Alexander Polishchuk and Leonid Positselski. *Quadratic algebras*, volume 37 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2005.

[She80] James B. Shearer. A graded algebra with a nonrational Hilbert series. *J. Algebra*, 62(1):228–231, 1980.

[Šir58] A. I. Širšov. On free Lie rings. *Mat. Sb. N.S.*, 45(87):113–122, 1958.

[Šir62] A. I. Širšov. On the bases of a free Lie algebra. *Algebra i Logika Sem.*, 1(1):14–19, 1962.

[Šme73] A. L. Šmel′kin. Wreath products of Lie algebras, and their application in group theory. *Trudy Moskov. Mat. Obšč.*, 29:247–260, 1973. Collection of articles commemorating Aleksandr Gennadievič Kuroš.

[Smi76] M. K. Smith. Universal enveloping algebras with subexponential but not polynomially bounded growth. *Proc. Amer. Math. Soc.*, 60(1):22–24, 1976.

[Sta97] Richard P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[Sta99] Richard P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.

[Ste75] Ian Stewart. Finitely presented infinite-dimensional simple Lie algebras. *Arch. Math. (Basel)*, 26(5):504–507, 1975.

[Šva55] A. S. Švarc. A volume invariant of coverings. *Dokl. Akad. Nauk SSSR (N.S.)*, 105:32–34, 1955.

[Ufn80] V. A. Ufnarovskiĭ. Poincaré series of graded algebras. *Mat. Zametki*, 27(1):21–32, 157, 1980.

[Ufn82] V. A. Ufnarovskiĭ. Criterion for the growth of graphs and algebras given by words. *Mat. Zametki*, 31(3):465–472, 476, 1982.

[Ufn90] V. A. Ufnarovskiĭ. Combinatorial and asymptotic methods in algebra. In *Current problems in mathematics. Fundamental directions, Vol. 57 (Rus-*

sian), Itogi Nauki i Tekhniki, pages 5–177. Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1990.

[Wol68] Joseph A. Wolf. Growth of finitely generated solvable groups and curvature of Riemanniann manifolds. *J. Differential Geometry*, 2:421–446, 1968.

[Zas64] A. H. Zaslavskiĭ. On the isomorphism problem for stationary processes. *Teor. Verojatnost. i Primenen.*, 9:318–326, 1964.

APPENDIX A

A PRESENTATION OF THE VERONESE SUBALGEBRA OF $U(L)$

Let $U = U(L)$ be an associative algebra with generators x, y and the set of relations $R = \{x^3y - 3x^2yx + 3xyx^2 - yx^3 = 0,\ y^3x - 3y^2xy + 3yxy^2 - xy^3 = 0\}$ as in Theorem 3.1.1. Since R is a set of two homogeneous polynomials, U is a graded algebra. Let $V_4(U)$ be the Veronese subalgebra of U . It was proven in Section 3.2 that $V_4(U)$ is a graded algebra generated by the set S of monomials of length 4 over $\{x, y\}$ and the set of relations $R^* = \{f_i = 0, vf_iw = 0\}$ where v, w are monomials such that $l(v)+l(w) = 4$ and, $f_1 = x^3y-3x^2yx+3xyx^2-yx^3,\ f_2 = y^3x-3y^2xy+3yxy^2-xy^3$. Basically, R^* is the set of homogeneous polynomials of degree 4 or 8 generated by $R = \{f_1 = 0, f_2 = 0\}$ in $k[x, y]$. Since there are 48 different pairs (v, w) of monomials, R^* consists of 2 homogeneous polynomials of degree 4:

$$(i)\ yx^3 = x^3y - 3x^2yx + 3xyx^2,\ \ (ii)\ y^3x = xy^3 - 3yxy^2 + 3y^2xy$$

and 96 homogeneous polynomials of degree 8:

(1) $xyx^2x^4 = x^4yx^3 - 3x^3yx^4 + 3x^2yxx^4$,

(2) $x^3yx^4 = x^4x^2yx - 3x^4xyx^2 + 3x^4yx^3$,

(3) $x^2y^2yx^3 = x^3yy^2x^2 - 3x^2yxy^2x^2 + 3x^2y^2xyx^2$,

(4) $xyx^2x^3y = x^4yx^2y - 3x^3yx^3y + 3x^2yxx^3y$,

(5) $x^3yx^3y = x^4x^2y^2 - 3x^4xyxy + 3x^4yx^2y$,

(6) $x^2y^2yx^2y = x^3yy^2xy - 3x^2yxy^2xy + 3x^2y^2xyxy$,

(7) $xyx^2x^2yx = x^4yxyx - 3x^3yx^2yx + 3x^2yxx^2yx$,

(8) $x^2y^2x^4 = x^2yxx^2yx - 3x^2yxxyx^2 + 3x^2yxyx^3$,

(9) $x^2y^2yxyx = x^3yy^3x - 3x^2yxy^3x + 3x^2y^2xy^2x$,

(10) $xyx^2x^2y^2 = x^4yxy^2 - 3x^3yx^2y^2 + 3x^2yxx^2y^2$,

(11) $x^2y^2x^3y = x^2yxx^2y^2 - 3x^2yxxyxy + 3x^2yxyx^2y$,

(12) $x^2y^2yxy^2 = x^3yy^4 - 3x^2yxy^4 + 3x^2y^2xy^3$,

(13) $xyx^2xyx^2 = x^4y^2x^2 - 3x^3yxyx^2 + 3x^2yxxyx^2$,

(14) $xyxyx^4 = xyx^2x^2yx - 3xyx^2xyx^2 + 3xyx^2yx^3$,

(15) $xy^3yx^3 = xyxyy^2x^2 - 3xy^2xy^2x^2 + 3xy^3xyx^2$,

(16) $xyx^2xy^2x = x^4y^3x - 3x^3yxy^2x + 3x^2yxxy^2x$,

(17) $xy^3x^4 = xy^2xx^2yx - 3xy^2xxyx^2 + 3xy^2xyx^3$,

(18) $xy^3yxyx = xyxyy^3x - 3xy^2xy^3x + 3xy^3xy^2x$,

(19) $xyx^2xyxy = x^4y^2xy - 3x^3yxyxy + 3x^2yxxyxy$,

(20) $xyxyx^3y = xyx^2x^2y^2 - 3xyx^2xyxy + 3xyx^2yx^2y$,

(21) $xy^3yx^2y = xyxyy^2xy - 3xy^2xy^2xy + 3xy^3xyxy$,

(22) $xyx^2xy^3 = x^4y^4 - 3x^3yxy^3 + 3x^2yxxy^3$,

(23) $xy^3x^3y = xy^2xx^2y^2 - 3xy^2xxyxy + 3xy^2xyx^2y$,

(24) $xy^3yxy^2 = xyxyy^4 - 3xy^2xy^4 + 3xy^3xy^3$,

(25) $y^2x^2x^4 = yx^3yx^3 - 3yx^2yx^4 + 3yxyxx^4$,

(26) $yx^2yx^4 = yx^3x^2yx - 3yx^3xyx^2 + 3yx^3yx^3$,

(27) $yxy^2yx^3 = yx^2yy^2x^2 - 3yxyxy^2x^2 + 3yxy^2xyx^2$,

(28) $x^2y^2x^2yx = yx^3yxyx - 3yx^2yx^2yx + 3yxyxy^2xy$,

(29) $yxy^2x^4 = yxyxx^2yx - 3yxyxxyx^2 + 3yxyxyx^3$,

(30) $yxy^2yxyx = yx^2yy^3x - 3yxyxy^3x + 3yxy^2xy^2x$,

(31) $y^2x^2x^2y^2 = yx^3yxy^2 - 3yx^2yx^2y^2 + 3yxyxx^2y^2$,

(32) $yxy^2x^3y = yxyxx^2y^2 - 3yxyxxyxy + 3yxyxyx^2y$,

(33) $yxy^2yxy^2 = yx^2yy^4 - 3yxyxy^4 + 3yxy^2xy^3$,

(34) $y^2x^2x^3y = yx^3yx^2y - 3yx^2yx^3y + 3yxyxx^3y$,

(35) $yx^2yx^3y = yx^3x^2y^2 - 3yx^3xyxy + 3yx^3yx^2y$,

(36) $yxy^2yx^2y = yx^2yy^2xy - 3yxyxy^2xy + 3yxy^2xyxy,$

(37) $y^2x^2xyx^2 = yx^3y^2x^2 - 3yx^2yxyx^2 + 3yxyxxyx^2,$

(38) $y^2xyx^4 = y^2x^2x^2yx - 3y^2x^2xyx^2 + 3y^2x^2yx^3,$

(39) $y^4yx^3 = y^2xyy^2x^2 - 3y^3xy^2x^2 + 3y^4xyx^2,$

(40) $y^2x^2xyxy = yx^3y^2xy - 3yx^2yxyxy + 3yxyxxyxy,$

(41) $y^2xyx^3y = y^2x^2x^2y^2 - 3y^2x^2xyxy + 3y^2x^2yx^2y,$

(42) $y^4yx^2y = y^2xyy^2xy - 3y^3xy^2xy + 3y^4xyxy,$

(43) $y^2x^2xy^2x = yx^3y^3x - 3yx^2yxy^2x + 3yxyxxy^2x,$

(44) $y^4x^4 = y^3xx^2yx - 3y^3xxyx^2 + 3y^3xyx^3,$

(45) $y^4yxyx = y^2xyy^3x - 3y^3xy^3x + 3y^4xy^2x,$

(46) $y^2x^2xy^3 = yx^3y^4 - 3yx^2yxy^3 + 3yxyxxy^3,$

(47) $y^4x^3y = y^3xx^2y^2 - 3y^3xxyxy + 3y^3xyx^2y,$

(48) $y^4yxy^2 = y^2xyy^4 - 3y^3xy^4 + 3y^4xy^3,$

(49) $x^2yxx^4 = x^4xyx^2 - 3x^4yx^3 + 3x^3yx^4,$

(50) $xy^3x^4 = x^2y^2yx^3 - 3xyxyyx^3 + 3xy^2xyx^3,$

(51) $x^3yy^2x^2 = x^4y^3x - 3x^3yxy^2x + 3x^3yyxyx,$

(52) $x^2yxx^3y = x^4xyxy - 3x^4yx^2y + 3x^3yx^3y,$

(53) $xy^3x^3y = x^2y^2yx^2y - 3xyxyyx^2y + 3xy^2xyx^2y,$

(54) $x^3yy^2xy = x^4y^4 - 3x^3yxy^3 + 3x^3yyxy^2,$

(55) $x^2yxx^2yx = x^4xy^2x - 3x^4yxyx + 3x^3yx^2yx,$

(56) $xy^3x^2yx = x^2y^2yxyx - 3xyxyyxyx + 3xy^2xyxyx,$

(57) $x^2y^2y^2x^2 = x^2yxy^3x - 3x^2y^2xy^2x + 3x^2y^2yxyx,$

(58) $x^2yxx^2y^2 = x^4xy^3 - 3x^4yxy^2 + 3x^3yx^2y^2,$

(59) $xy^3x^2y^2 = x^2y^2yxy^2 - 3xyxyyxy^2 + 3xy^2xyxy^2,$

(60) $x^2y^2y^2xy = x^2yxy^4 - 3x^2y^2xy^3 + 3x^2y^2yxy^2,$

(61) $xy^2xx^4 = xyx^2xyx^2 - 3xyx^2yx^3 + 3xyxyx^4,$

(62) $xy^3xyx^2 = x^2y^2y^2x^2 - 3xyxyy^2x^2 + 3xy^2xy^2x^2,$

(62) $xy^3xyx^2 = x^2y^2y^2x^2 - 3xyxyy^2x^2 + 3xy^2xy^2x^2$,

(63) $xyxyy^2x^2 = xyx^2y^3x - 3xyxyxy^2x + 3xyxyyxyx$,

(64) $xy^2xx^2yx = xyx^2xy^2x - 3xyx^2yxyx + 3xyxyx^2yx$,

(65) $xy^3xy^2x = x^2y^2y^3x - 3xyxyy^3x + 3xy^2xy^3x$,

(66) $xy^3y^2x^2 = xy^2xy^3x - 3xy^3xy^2x + 3xy^3yxyx$,

(67) $xy^2xx^3y = xyx^2xyxy - 3xyx^2yx^2y + 3xyxyx^3y$,

(68) $xy^3xyxy = x^2y^2y^2xy - 3xyxyy^2xy + 3xy^2xy^2xy$,

(69) $xyxyy^2xy = xyx^2y^4 - 3xyxyxy^3 + 3xyxyyxy^2$,

(70) $xy^2xx^2y^2 = xyx^2xy^3 - 3xyx^2yxy^2 + 3xyxyx^2y^2$,

(71) $xy^3xy^3 = x^2y^2y^4 - 3xyxyy^4 + 3xy^2xy^4$,

(72) $xy^3y^2xy = xy^2xy^4 - 3xy^3xy^3 + 3xy^3yxy^2$,

(73) $yxyxx^4 = yx^3xyx^2 - 3yx^3yx^3 + 3yx^2yx^4$,

(74) $y^4x^4 = yxy^2yx^3 - 3y^2xyyx^3 + 3y^3xyx^3$,

(75) $yx^2yy^2x^2 = yx^3y^3x - 3yx^2yxy^2x + 3yx^2yyxyx$,

(76) $yxyxx^2yx = yx^3xy^2x - 3yx^3yxyx + 3yx^2yx^2yx$,

(77) $y^4x^2yx = yxy^2yxyx - 3y^2xyyxyx + 3y^3xyxyx$,

(78) $yxy^2y^2x^2 = yxyxy^3x - 3yxy^2xy^2x + 3yxy^2yxyx$,

(79) $yxyxx^2y^2 = yx^3xy^3 - 3yx^3yxy^2 + 3yx^2yx^2y^2$,

(80) $y^4x^2y^2 = yxy^2yxy^2 - 3y^2xyyxy^2 + 3y^3xyxy^2$,

(81) $yxy^2y^2xy = yxyxy^4 - 3yxy^2xy^3 + 3yxy^2yxy^2$,

(82) $yxyxx^3y = yx^3xyxy - 3yx^3yx^2y + 3yx^2yx^3y$,

(84) $yx^2yy^2xy = yx^3y^4 - 3yx^2yxy^3 + 3yx^2yyxy^2$,

(85) $y^3xx^4 = y^2x^2xyx^2 - 3y^2x^2yx^3 - 3y^2xyx^4$,

(86) $y^4xyx^2 = yxy^2y^2x^2 - 3y^2xyy^2x^2 + 3y^3xy^2x^2$,

(87) $y^2xyy^2x^2 = y^2x^2y^3x - 3y^2xyxy^2x + 3y^2xyyxyx$,

(88) $y^3xx^3y = y^2x^2xyxy - 3y^2x^2yx^2y + 3y^2xyx^3y$,

(89) $y^4xyxy = yxy^2y^2xy - 3y^2xyy^2xy + 3y^3xy^2xy$,

(90) $y^2xyy^2xy = y^2x^2y^4 - 3y^2xyxy^3 + 3y^2xyyxy^2$,

(91) $y^3xx^2yx = y^2x^2yx^2x - 3y^2x^2yxyx + 3y^2xyx^2yx$,

(92) $y^4xy^2x = yxy^2y^3x - 3y^2xyy^3x + 3y^3xy^3x$,

(93) $y^4y^2x^2 = y^3xy^3x - 3y^4xy^2x + 3y^4yxyx$,

(94) $y^3xx^2y^2 = y^2x^2xy^3 - 3y^2x^2yxy^2 + 3y^2xyx^2y^2$,

(95) $y^4xy^3 = yxy^2y^4 - 3y^2xyy^4 - 3y^2xyy^4 + 3y^3xy^4$,

(96) $y^4y^2xy = y^3xy^4 - 3y^4xy^3 + 3y^4yxy^2$.

We can rename the generators as follows: $y^4 = Y_1,\ y^3x = Y_2,\ y^2xy = Y_3,\ y^2x^2 = Y_4,\ yxy^2 = Y_5,\ yxyx = Y_6, yx^2y = Y_7,\ yx^3 = Y_8,\ xy^3 = X_1,\ xy^2x = X_2,\ xyxy = X_3,\ xyx^2 = X_4,\ x^2y^2 = X_5,\ x^2yx = X_6,\ x^3y = X_7,\ x^4 = X_8$. So the relations will be

$$(i)\ Y_8 = X_7 - 3X_6 + 3X_4,\ \ (ii)\ Y_2 = X_1 - 3Y_5 + 3Y_3$$

(1) $X_4X_8 = X_8Y_8 - 3X_7X_8 + 3X_6X_8$,

(2) $X_7X_8 = X_8X_6 - 3X_8X_4 + 3X_8Y_8$,

(3) $X_5Y_8 = X_7Y_4 - 3X_6Y_4 + 3X_5X_4$,

(4) $X_4X_7 = X_8Y_7 - 3X_7X_7 + 3X_6X_7$,

(5) $X_7X_7 = X_8X_5 - 3X_8X_3 + 3X_8Y_7$,

(6) $X_5Y_7 = X_7Y_3 - 3X_6Y_3 + 3X_5X_3$,

(7) $X_4X_6 = X_8Y_6 - 3X_7X_6 + 3X_6X_6$,

(8) $X_5X_8 = X_6X_6 - 3X_6X_4 + 3X_6Y_8$,

(9) $X_5Y_6 = X_7Y_2 - 3X_6Y_2 + 3X_5X_2$,

(10) $X_4X_5 = X_8Y_5 - 3X_7X_5 + 3X_6X_5$,

(11) $X_5X_7 = X_6X_5 - 3X_6X_3 + 3X_6Y_7$,

(12) $X_5Y_5 = X_7Y_1 - 3X_6Y_1 + 3X_5X_1$,

(13) $X_4X_4 = X_8Y_4 - 3X_7X_4 + 3X_6X_4$,

(49) $X_6X_8 = X_8X_4 - 3X_8Y_8 + 3X_7X_8$,

(50) $X_1X_8 = X_5Y_8 - 3X_3Y_8 + 3X_2Y_8$,

(51) $X_7Y_4 = X_8Y_2 - 3X_7X_2 + 3X_7Y_6$,

(52) $X_6X_7 = X_8X_3 - 3X_8Y_7 + 3X_7X_7$,

(53) $X_1X_7 = X_5Y_7 - 3X_3Y_7 + 3X_2Y_7$,

(54) $X_7Y_3 = X_8Y_1 - 3X_7X_1 + 3X_7Y_5$,

(55) $X_6X_6 = X_8X_2 - 3X_8Y_6 + 3X_7X_6$,

(56) $X_1X_6 = X_5Y_6 - 3X_3Y_6 + 3X_2Y_6$,

(57) $X_5Y_4 = X_6Y_2 - 3X_5X_2 + 3X_5Y_6$,

(58) $, X_6X_5 = X_8X_1 - 3X_8Y_5 + 3X_7X_5$,

(59) $X_1X_5 = X_5Y_5 - 3X_3Y_5 + 3X_2Y_5$,

(60) $X_5Y_3 = X_6Y_1 - 3X_5X_1 + 3X_5Y_5$,

(61) $X_2X_8 = X_4X_4 - 3X_4Y_8 + 3X_3X_8$,

(14) $X_3X_8 = X_4X_6 - 3X_4X_4 + 3X_4Y_8$,
(15) $X_1Y_8 = X_3Y_4 - 3X_2Y_4 + 3X_1X_4$,
(16) $X_4X_2 = X_8Y_2 - 3X_7X_2 + 3X_6X_2$,
(17) $X_1X_8 = X_2X_6 - 3X_2X_4 + 3X_2Y_8$,
(18) $X_1Y_6 = X_3Y_2 - 3X_2Y_2 + 3X_1X_2$,
(19) $X_4X_3 = X_8Y_3 - 3X_7X_3 + 3X_6X_3$,
(20) $X_3X_7 = X_4X_5 - 3X_4X_3 + 3X_4Y_7$,
(21) $X_1Y_7 = X_3Y_3 - 3X_2Y_3 + 3X_1X_3$,
(22) $X_4X_1 = X_8Y_1 - 3X_7X_1 + 3X_6X_1$,
(23) $X_1X_7 = X_2X_5 - 3X_2X_3 + 3X_2Y_7$,
(24) $X_1Y_5 = X_3Y_1 - 3X_2Y_1 + 3X_1X_1$,
(25) $Y_4X_8 = Y_8Y_8 - 3Y_7X_8 + 3Y_6X_8$,
(26) $Y_7X_8 = Y_8X_6 - 3Y_8X_4 + 3Y_8Y_8$,
(27) $Y_5Y_8 = Y_7Y_4 - 3Y_6Y_4 + 3Y_5X_4$,
(28) $Y_4X_6 = Y_8Y_6 - 3Y_7X_6 + 3Y_6X_6$,
(29) $Y_5X_8 = Y_6X_6 - 3Y_6X_4 + 3Y_6Y_8$,
(30) $Y_5Y_6 = Y_7Y_2 - 3Y_6Y_2 + 3Y_5X_2$,
(31) $Y_4X_5 = Y_8Y_5 - 3Y_7X_5 + 3Y_6X_5$,
(32) $Y_5X_7 = Y_6X_5 - 3Y_6X_3 + 3Y_6Y_7$,
(33) $Y_5Y_5 = Y_7Y_1 - 3Y_6Y_1 + 3Y_5X_1$,
(34) $Y_4X_7 = Y_8Y_7 - 3Y_7X_7 + 3Y_6X_7$,
(35) $Y_7X_7 = Y_8X_5 - 3Y_8X_3 + 3Y_8Y_7$,
(36) $Y_5Y_7 = Y_7Y_3 - 3Y_6Y_3 + 3Y_5X_3$,
(37) $Y_4X_4 = Y_8Y_4 - 3Y_7X_4 + 3Y_6X_4$,
(38) $Y_3X_8 = Y_4X_6 - 3Y_4X_4 + 3Y_4Y_8$,
(39) $Y_1Y_8 = Y_3Y_4 - 3Y_2Y_4 + 3Y_1X_4$,
(40) $Y_4X_3 = Y_8Y_3 - 3Y_7X_3 + 3Y_6X_3$,
(62) $X_1X_4 = X_5Y_4 - 3X_3Y_4 + 3X_2Y_4$,
(63) $X_3Y_4 = X_4Y_2 - 3X_3X_2 + 3X_3Y_6$,
(64) $X_2X_6 = X_4X_2 - 3X_4Y_6 + 3X_3X_6$,
(65) $X_1X_2 = X_5Y_2 - 3X_3Y_2 + 3X_2Y_2$,
(66) $X_1Y_4 = X_2Y_2 - 3X_1X_2 + 3X_1Y_6$,
(67) $X_2X_7 = X_4X_3 - 3X_4Y_7 + 3X_3X_7$,
(68) $X_1X_3 = X_5Y_3 - 3X_3Y_3 + 3X_2Y_2$,
(69) $X_3Y_3 = X_4Y_1 - 3X_3X_1 + 3X_3Y_5$,
(70) $X_2X_5 = X_4X_1 - 3X_4Y_5 + 3X_3X_5$,
(71) $X_1X_1 = X_5Y_1 - 3X_3Y_1 + 3X_2Y_1$,
(72) $X_1Y_3 = X_2Y_1 - 3X_1X_1 + 3X_1Y_5$,
(73) $Y_6X_8 = Y_8X_4 - 3Y_8Y_8 + 3Y_7X_8$,
(74) $Y_1X_8 = Y_5Y_8 - 3Y_3Y_8 + 3Y_2Y_8$,
(75) $Y_7Y_4 = Y_8Y_2 - 3Y_7X_2 + 3Y_7Y_6$,
(76) $Y_6X_6 = Y_8X_2 - 3Y_8Y_6 + 3Y_7X_6$,
(77) $Y_1X_6 = Y_5Y_6 - 3Y_3Y_6 + 3Y_2Y_6$,
(78) $Y_5Y_4 = Y_6Y_2 - 3Y_5X_2 + 3Y_5Y_6$,
(79) $Y_6X_5 = Y_8X_1 - 3Y_8Y_5 + 3Y_7X_5$
(80) $Y_1X_5 = Y_5Y_5 - 3Y_3Y_5 + 3Y_2Y_5$,
(81) $Y_5Y_3 = Y_6Y_1 - 3Y_5X_1 + 3Y_5Y_5$,
(82) $Y_6X_7 = Y_8X_3 - 3Y_8Y_7 + 3Y_7X_7$,
(83) $Y_1X_7 = Y_5Y_7 - 3Y_3Y_7 + 3Y_2Y_7$,
(84) $Y_7Y_3 = Y_8Y_1 - 3Y_7X_1 + 3Y_7Y_5$,
(85) $Y_2X_8 = Y_4X_4 - 3Y_4Y_8 + 3Y_3X_8$,
(86) $Y_1X_4 = Y_5Y_4 - 3Y_3Y_4 + 3Y_2Y_4$,
(87) $Y_3Y_4 = Y_4Y_2 - 3Y_3X_2 + 3Y_3Y_6$,
(88) $Y_2X_7 = Y_4X_3 - 3Y_4Y_7 + 3Y_3X_7$,

(41) $Y_3X_7 = Y_4X_5 - 3Y_4X_3 + 3Y_4Y_7$, (89) $Y_1X_3 = Y_5Y_3 - 3Y_3Y_3 + 3Y_2Y_3$,

(42) $Y_1Y_7 = Y_3Y_3 - 3Y_2Y_3 + 3Y_1X_3$, (90) $Y_3Y_3 = Y_4Y_1 - 3Y_3X_1 + 3Y_3Y_5$,

(43) $Y_4X_2 = Y_8Y_2 - 3Y_7X_2 + 3Y_6X_2$, (91) $Y_2X_6 = Y_4X_2 - 3Y_4Y_6 + 3Y_3X_6$,

(44) $Y_1X_8 = Y_2X_6 - 3Y_2X_4 + 3Y_2Y_8$, (92) $Y_1X_2 = X_5Y_2 - 3Y_3Y_2 + 3Y_2Y_2$,

(45) $Y_1Y_6 = Y_3Y_2 - 3Y_2Y_2 + 3Y_1X_2$, (93) $Y_1Y_4 = Y_2Y_2 - 3Y_1X_2 + 3Y_1Y_6$,

(46) $Y_4X_1 = Y_8Y_1 - 3Y_7X_1 + 3Y_6X_1$, (94) $Y_2X_5 = Y_4X_1 - 3Y_4Y_5 + 3Y_3X_5$,

(47) $Y_1X_7 = Y_2X_5 - 3Y_2X_3 + 3Y_2Y_7$, (95) $Y_1X_1 = Y_5Y_1 - 3Y_3Y_1 + 3Y_2Y_1$,

(48) $Y_1Y_5 = Y_3Y_1 - 3Y_2Y_1 + 3Y_1X_1$, (96) $Y_1Y_3 = Y_2Y_1 - 3Y_1X_1 + 3Y_1Y_5$.

We see that $V_4(U)$ is a quadratic algebra with generators $X_1, \ldots, X_8, Y_1, \ldots Y_8$ and relations $(i), (ii)$, $(1) - (96)$. This may not be the simplest presentation of $V_4(U)$. Observe that the generators Y_8 and Y_2 are linear combinations of other generators by (i) and (ii), so they can be removed from the generating set.